ANNOUNCEMENT

regarding the organization of an open tender

The text of this Announcement has been approved by the Tender Committee of the Central Bank of Armenia's Protocol No. 52 dated 18th of December, 2025.

The Central Bank of Armenia announces a Tender, the terms of which are presented in the attached Invitation.

Issued on:	**30.12.2025թ.**
Procuring entity:	**Central Bank of Armenia** 6 Vazgen Sargsyan St., Yerevan, 0010, Armenia
Procedure Reference Number:	**CBA-2025-064**
Purpose of Procedure:	**Acquisition of a Real-Time Gross Settlement (RTGS) system**
Publication place:	**https://www.cba.am/en/SitePages/tenders.aspx**
Deadline for Submission of Proposals:	**Thursday, the 26th of February, 2026, not later than 4:00 p.m. (GMT+4)**
Submission method:	In electronic form, by sending an e-mail to the following address: **CBA-2025-064@cba.am**
Deadline for Requests for Clarifications of the Invitation:	**Wednesday, the 18th of February, 2026, not later than 4:00 p.m. (GMT+4)**
Date of Opening of Proposals:	**Thursday, the 26th of February, 2026, 4:00 p.m. (GMT+4)**
Notification of Award:	**Thursday, the 23th of April, 2026, 4:00 p.m. (GMT+4)**
Tender Organized By:	Central Bank of Armenia, Procurement Coordination Service
Communication method:	**In written form only:** Attention to: Ms. Siran Yeganyan, Head of Procuremer Coordination Service, Central Bank of the Republic of Armenia E-mail to: **siran.yeganyan@cba.am** cc: **procurement@cba.am**

The Bidder selected through this procedure will be offered a contract for the supply and implementation of the Real-Time Gross Settlement (RTGS) system and a contract for post-implementation support and related services.

INVITATION TO AN OPEN TENDER

Request for Proposals

FOR ACQUISITION OF THE REAL-TIME GROSS SETTLEMENT SYSTEM FOR THE NEEDS OF THE CENTRAL BANK OF THE REPUBLIC OF ARMENIA

CENTRAL BANK OF ARMENIA
6 Vazgen Sargsyan St., Yerevan, 0010, Armenia
Tel.: +374 10 592 592, www.cba.am

TABLE OF CONTENTS

1. DESCRIPTION OF SUBJECT OF PROCUREMENT 1
2. BIDDER PARTICIPATION REQUIREMENTS AND QUALIFICATION CRITERIA 1
3. PROPOSAL SUBMISSION PROCEDURE 4
4. PRICE PROPOSAL 7
5. CLARIFICATION OF INVITATION AND PROCEDURE FOR MAKING CHANGES TO THE INVITATION 8
6. OPENING, EVALUATION OF PROPOSALS AND NOTIFICATION OF AWARD 9
7. BID SECURITY 13
8. CONTRACT PERFORMANCE AND ADVANCE PAYMENT SECURITIES 14
9. EXECUTION OF THE CONTRACT 16
10. DECLARING THE PROCEDURE INVALID 17
11. BIDDERS' APPEAL RIGHTS 18

Appendix 1 19
Appendix 2 97
Appendix 2.1 100
Appendix 3 106
Appendix 3.1 107
Appendix 3.2 108
Appendix 4 110
Appendix 5 112
Appendix 6 113

This invitation is issued in addition to the Announcement of an Open tender (hereinafter also referred to as the "procedure") conducted under reference number CBA-2025-064.

This invitation has been prepared in accordance with the legislation of the Republic of Armenia, including the Law of the Republic of Armenia "On Procurements" (hereinafter referred to as the Law), and other applicable legal acts.

Within the scope of this procedure, payments for subscription licenses and technical support services for the subsequent years shall be organized in accordance with the requirements of Article 15 part 6 of the Law of the Republic of Armenia "On Procurement".

The execution of payments for services in each subsequent fiscal year, as stipulated in the Contract, shall be subject to the allocation of the relevant financial resources.

If such financial allocations are confirmed, the Contract remains in force. If they are not confirmed, the Procuring Entity shall notify the Supplier in advance, within the timeframes defined by the Contract. In such cases, the Supplier shall not be obligated to provide services, and the Procuring Entity shall not be obligated to pay for them.

In the absence of allocated financial resources, the Procuring Entity reserves the right to unilaterally terminate the performance of the Contract.

All persons, including foreign individuals or organizations and stateless persons, are eligible to submit Proposals.

The Procuring Entity reserves the right to disregard in the contract any condition (or other information/data) in the proposal that is not expressly stipulated in this Invitation.

All matters related to this procedure shall be governed by the laws of the Republic of Armenia. Any disputes arising in connection with this procedure shall be examined and resolved by the courts of the Republic of Armenia.

The e-mail address of the Secretary of the Tender Committee is: siran.yeganyan@cba.am.

1. DESCRIPTION OF SUBJECT OF PROCUREMENT

1.1. The subject of procurement is the implementation of the RTGS system for the needs of the Central Bank of the Republic of Armenia (hereinafter referred as "Purchaser").

1.2. The purpose of this Request for Proposal (RFP) is to invite qualified solution providers to submit comprehensive proposals for the modernization of the national financial market infrastructure. This modernization will include the implementation of secure, highly resilient, interoperable, and future-ready central bank RTGS system that provides safe real-time settlement in central bank money while supporting wider access and ISO 20022 data richness.

Through this RFP, the Central Bank of Armenia seeks to engage experienced, capable, and innovative firms with a strong track record in implementing ISO 20022-compliant RTGS and high-value payment infrastructures, and delivering secure, resilient, and scalable architectures designed for mission-critical financial systems.

1.3. In accordance with this procedure, the procurement shall be carried out in a total of 1 (one) Lot.

1.4. The Terms of Reference (ToR), attached as per Appendix 1, form an inseparable part of this RFP and establish the minimum technical, functional, non-functional, and security requirements applicable to the solution. All requirements in the ToR must be fully addressed in the Bidder's proposal. These requirements shall be included in and shall govern the execution of the Contract.

2. BIDDER PARTICIPATION REQUIREMENTS AND QUALIFICATION CRITERIA

2.1. The following persons shall not be eligible to participate in this procedure:

1) Persons who have been declared bankrupt by a court as of the date of submission of the Proposal.

2) Persons who, or whose executive body representative, have been convicted within the 5 (five) years preceding the date of submission of the Proposal of financing terrorism, crimes involving child exploitation or human trafficking, creating or participating in a criminal partnership, receiving, giving or brokering bribes, or crimes against economic activity as defined by law, except where the conviction has been removed or extinguished in accordance with the law.

3) Persons in respect of whom an administrative act establishing liability for anti-competitive agreements, abuse of dominant position, or unfair competition in the field of procurement became final within the 3 (three) years preceding the date of submission of the Proposal, or was upheld in the event of an appeal.

4) Persons who, as of the date of submission of the Proposal, are included in the list of bidders prohibited from participating in procurement processes, published in accordance with the procurement legislation of the member states of the Eurasian Economic Union. The condition does not apply to procurement processes financed under international agreements.

5) Persons who, as of the date of submission of the Proposal, are included in the list of bidders prohibited from participating in the procurement process.

   If a bidder is included in the list referred to in sub-clauses 4 and 5 of this clause after the date of submission of the Proposal, the Proposal shall not be subject to rejection on this ground.

   A bidder may be included in the aforementioned list if the bidder:

   - violated a contractual obligation or an obligation assumed within the framework of a procurement process, resulting in unilateral termination of the contract by the Purchaser, termination of the bidder's right to further participate in the procurement process, or failure to pay the prepayment, contract performance security, and/or qualification security amount within the period specified in the invitation or contract;

     or

   - refused to execute a contract as the selected bidder or was deprived of the right to execute the contract.

2.2. To assess a bidder's eligibility to participate, together with the proposal, a written statement must be provided approved by the bidder in accordance with clause 2.1 of Part 2 of this invitation. No other documents or justifications may be required from the bidder, including from the selected bidder, for the assessment of eligibility. The authenticity of the bidder's statement shall be evaluated by the Tender Committee (hereinafter referred to as the "Committee") under the conditions set forth in this invitation.

2.3. Inclusion of a bidder in the list referred to in sub-clause 5 of clause 2.1 of Part 2 of this invitation automatically results in the restriction of the right of affiliated persons to participate in the procurement process for the duration of the bidder's inclusion in the list.

2.4. Simultaneous participation in this procedure of affiliated persons as defined in this clause, and/or organizations founded by the same person(s) or with more than 50 % (fifty percent) ownership by the same person(s), is prohibited, except in cases of participation by state or municipalities-founded organization and/or through a joint venture (JV) or consortium.

2.5. A bidder who declared the selected bidder shall provide a contract performance security in the manner and amount specified in this Invitation.

The Purchaser may waive the requirement to provide a contract performance security if, as of the date of Proposal opening, the selected bidder, or the organization providing services under this procedure as its officially authorized representative holds a credit rating equal to or higher than the sovereign credit rating of the Republic of Armenia, as assigned by a reputable international credit rating agency (such as Fitch Ratings, Moody's Investor Services, or S&P Global Ratings).

2.6. Bidders can participate in this procedure as joint ventures (consortium or JV). In such cases:

1) the Proposal shall include a joint venture agreement.
2) the joint venture shall nominate an Authorized representative who shall have the authority to conduct all business for and on behalf of any and all the members of the JV during the bidding process and, in the event the JV is awarded the Contract, during contract execution.
3) the Proposal shall be signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a Power of Attorney signed by their legally authorized representatives.
4) during evaluation, the combined qualifications of all members to the joint venture shall be taken into account.
5) participants shall bear joint and several liability. If a consortium member withdraws, the contract concluded by the Purchaser with the consortium shall be unilaterally terminated, and the liability measures stipulated in the contract shall apply to the consortium members.
6) any party to the joint venture agreement may not submit a separate Proposal for the same procedure. Failure to comply with this requirement will result in the rejection of both joint venture Proposal and the separately submitted Proposal(s) at the Proposal opening session.

2.7. The bidder must demonstrate adequate experience, technical capability, and resources to fully perform the contractual obligations. The eligibility and qualification criteria are defined in Terms of Reference as per Appendix 1 to this Invitation. Only proposals that meet the following minimum qualification requirement shall be shortlisted for further evaluation:

2.7.1. The criterion of **"Professional experience"** will be evaluated as follows:

- The bidder must have a minimum of 5 (five) years of proven experience in the design and implementation of RTGS solutions for central banks.
- The bidder must have successfully completed at least 3 (three) contracts of a similar nature and scope within the last 10 years. The bidder must have at least 3 (three) existing support & maintenance contract.

2.7.2. The bidders failing to meet the minimum qualification requirement will be disqualified.

3. PROPOSAL SUBMISSION PROCEDURE

3.1. To participate in this procedure, a bidder must submit a Proposal to the Committee. A Proposal is an offer submitted by the bidder based on this Invitation.

3.2. Bidders may not submit more than one Proposal for the same procedure, except when submitting amendments to the Proposal provided for in clauses 3.9 and 5.7 of this Invitation.

3.3. Proposals must be submitted to the Committee no later than the Proposal submission deadline indicated in the announcement of this procedure.

3.4. Proposals must be submitted electronically to **CBA-2025-064@cba.am**.

Documents must be submitted either in signed printed (scanned) format or in PDF format with electronic digital signatures.

3.5. Proposals must be submitted in English.

3.6. When submitting a Proposal electronically, the following rules must be observed:

- The Reference Number "CBA-2025-064" must be included in the "Subject-line" of the e-mail.
- The proposal must be attached in **PDF format** only as one complete document, maintaining the order of documents specified in clause 3.11 of this Invitation.

- The attachments **must not** be submitted as a **Google Drive link, .rar file**, or in any similar link format.
- The total size of the email, including attachments, **must not exceed 25MB**. Bidders are responsible for ensuring that their electronic submissions comply with this limitation.
- If the files exceed the file size limit, the submission may be split into multiple emails, each clearly labeled (e.g., 'Part 1 of 3,' 'Part 2 of 3,' etc.).
- All attachments must be scanned for viruses prior to submission.
- The body of the email must contain plain text only and must not include any links.

Failures to comply with these rules may result in the Proposal being blocked by the Purchaser's virus protection system and not delivered. The Purchaser bears no responsibility in such cases.

Non-adherence may lead to the Proposal being deemed non-compliant and ineligible for evaluation.

It is strongly recommended that bidders submit their proposals at least 1-2 hours before the deadline to ensure timely delivery and to avoid potential technical issues.

An automatic confirmation email will be sent to the bidder upon receipt of the Proposal.

3.7. The Purchaser shall not be responsible for the receipt of emailed Proposals submitted after the deadline.

3.8. Proposals that do not comply with the requirements of Part 3 of this Invitation shall be rejected by the Committee at the Proposal opening session.

3.9. Bidders may amend or withdraw their Proposals before the Proposal submission deadline.

- In the event of an amendment, the revised Proposal must be sent to the email address specified in clause 3.4, following the procedure set out in this Part, with the subject line containing the phrase "Amendment to Proposal".
- To withdraw a Proposal, a notice of cancellation must be sent to **procurement@cba.am**.

3.10. **The bidder must submit the minimum set of following documents:**

1) An **application-statement** approved by the bidder in accordance with Appendix 2 to this Invitation, including:

a) a certification of compliance of the bidder and related persons with the participation requirements established by this Invitation,

b) a statement confirming the absence of unfair competition, abuse of a dominant position, and anti-competitive agreements within the scope of this procedure,

c) a statement confirming the absence of separate participation in the procedure by any persons affiliated with the bidder and/or organizations founded by or with more than 50% (fifty percent) ownership by the bidder,

d) a declaration of actual beneficiaries, in accordance with Appendix 2.1 to this Invitation (not required if the bidder is an individual entrepreneur or natural person).

2) A document confirming the **bid security** for participation in the tender,
3) The **financial proposal**, completed in accordance with Appendix 3 to this Invitation,
4) **Breakdown of the financial proposal,** completed in accordance with Appendix 3.1 and 3.2, including proposed payment terms and conditions,
5) **The technical proposal,** including the detailed description of the proposed solution, prepared in accordance with Appendix 4,
6) **Company Portfolio,** completed in accordance with Appendix 5,
7) **Organizational and Governance Overview,** completed in accordance with Appendix 6,
8) **The Financial Stability Report** – including financial statements for the past three (3) years (2022, 2023, and 2024) and interim financial reports for 2025. Please refer to Financial Stability requirement in Chapter 9.4 of the ToR for more details,
9) Any other supporting documents and information specified in Terms of Reference of this Invitation, including those that demonstrate the bidder's capacity, experience, or other qualifications supporting its proposal.
10) A **draft version of the contract** outlining the principal terms, conditions, responsibilities, and other relevant provisions (if available).

4. PRICE PROPOSAL

4.1. The proposed price, shall include, in addition to the cost of the Project, all expenses related to transportation, insurance, duties, taxes, and other charges, and may not be lower than their actual cost.

4.2. The bidder must submit the price proposal as a calculation consisting of the price (the sum of all costs) and the value-added tax ((VAT), applicable for resident bidders) for each Lot. If the bidder has to pay VAT to the state budget of the Republic of Armenia for the given transaction, the amount of VAT should be indicated separately.

4.3. The bidder must attach to the price proposal a detailed breakdown of the price of each component included in a given Lot.

4.4. The comparison of bidders' price proposals (Appendix 3) will be carried out excluding the amount of VAT mentioned in this clause.

The evaluation of the bidder's price proposal shall distinguish between material and non-material deviations. A proposal shall not be rejected on the basis of a non-material deviation. Non-material deviations include, but are not limited to, the following cases:

a. the "Price" and "VAT" columns of the price proposal are completed using numbers only, while the "Total Price" column is completed using both words and numbers or only words;

b. a discrepancy exists between the amounts stated in words or numerals in the "Price" and "VAT" columns, but the sum of any of the amounts indicated in either the words or numerals corresponds to the amount indicated in words in the "Total Price" column;

c. the Lot number is indicated incorrectly in the price proposal but the name of the purchase item is correctly filled in;

d. fractional monetary units in the "Price", "VAT", and "Total Price" columns are rounded down to the nearest whole number when below five-tenths and rounded up when at or above five-tenths;

e. The "Price" and "VAT" columns contain matching amounts in words and numerals, while the "Total Price" column contains extra words resulting in a non-existent or incorrect number – in this case, the Committee will base its assessment on the sum of the amounts written in words in the "Price" and "VAT" columns.

f. fractional monetary units of amounts written in words are indicated with numbers.

4.5. The proposal shall be rejected if it contains a material deviation, that alters or impacts the bidder's actual offered price, creates ambiguity in determining the price, or may influence the competitive ranking of bids.

4.6. The price proposal document as per Appendix 3 is not subject to correction.

4.7. The financial proposal for non-resident Bidders of the Republic of Armenia shall be expressed in United States Dollars or Euros. In such case, for Proposal evaluation and comparison purposes all prices expressed in foreign currency will be converted into Armenian Drams (AMD). The conversion shall be conducted by the Purchaser, with the exchange rate announced at its official website "**www.cba.am**" on the date of opening of Proposals. Moreover, a contract will be executed in the same currency as submitted in the proposal.

4.8. In the event that the contract is concluded with a non-resident of the Republic of Armenia, profit tax shall apply, calculated at a rate of twenty percent (20%) of the contract price and shall be paid by the Purchaser. The applicable tax rate may be subject to change in the presence of a Double Taxation Avoidance Agreement between the countries of the Purchaser and the Bidder. In such cases, the selected Bidder must submit a Certificate of Tax Residency issued by the tax authority of their country within ten (10) calendar days from the date of signing the contract.

4.9. If the bidder is subject to profit tax, the comparison of price proposals shall be carried out based on the total value including the profit tax.

5. CLARIFICATION OF INVITATION AND PROCEDURE FOR MAKING CHANGES TO THE INVITATION

5.1. Bidders may request clarifications from the Committee in writing, no later than the deadline specified for Clarification Requests under this Invitation by sending a request to **procurement@cba.am.**

5.2. Clarifications shall be provided to bidders who have submitted a written request within 2 (two) working days following the date of receipt of the request.

5.3. On the day the clarification is provided, the content of the request and the clarification shall also be published on the official website "**www.cba.am**" under the "Tenders" section, without disclosing the identity of the bidder who submitted the request.

5.4. Clarification shall not be provided if the request was submitted after the deadline specified in this section, if the request falls outside the scope of the Invitation, or if responding to the request would involve the risk of disclosing state secrets.

5.5. Clarification shall not be provided if the inquiry concerns the correspondence between the technical specifications proposed by the bidder and those stipulated in this Invitation.

5.6. Changes to the Invitation can be made up to 5 (five) working days before the proposal submission deadline. Within 3 (three) working days of such changes, an announcement detailing the modifications and their terms will be published on the official website "**www.cba.am**", under the "Tenders" section. In the event of changes to the Invitation, the proposal submission deadline shall be adjusted and recalculated, as appropriate, based on the date of issuance of the change notice and the nature of the modification.

5.7. If changes are made to the Invitation, bidders have the right to amend their proposals in accordance with the procedure set forth in this Invitation. The Purchaser shall not be liable for any losses incurred by bidders as a result of changes to the terms of the Invitation.

6. OPENING, EVALUATION OF PROPOSALS AND NOTIFICATION OF AWARD

6.1. The Committee's proposal opening session shall be convened at the Central Bank of the Republic of Armenia, 6 Vazgen Sargsyan St., Yerevan, on the date and time specified in the Announcement.

6.2. At the proposal opening session, the Committee shall evaluate:

- compliance with the procedure established by this Invitation for the electronic preparation and submission of proposals,
- the presence of the required documents in each proposal and their compliance with the requisites stipulated in the Invitation.

6.3. The Secretary of the Committee shall announce the price proposals of the bidders, expressed in a single number, based on the amount written in words.

6.4. The session for reviewing the results of the proposal evaluation shall be convened at the Central Bank of the Republic of Armenia, 6 Vazgen Sargsyan St., Yerevan, on the date and time specified in the Announcement.

6.5. The Committee may change the date and time of the notification of award by notifying the bidders.

6.6. Proposals shall be evaluated in accordance with this Invitation.

6.7. Proposals that meet the conditions set forth in this Invitation shall be deemed satisfactory; otherwise, they shall be deemed unsatisfactory and rejected. The Committee rejects proposals for which a price proposal is missing or presented inconsistently with the Invitation.

6.8. Proposals will be evaluated based on **non-financial** and **financial** criteria. The non-financial evaluation includes the bidder's **qualification criteria**, the **technical proposal**, and the **bidder's overall impression**, which together carry a total weight of **70%** (60 pp for the technical proposal and qualification criteria, 10 pp for the **bidder's overall** impression). The **financial proposal** carries a weight of **30%**. The contract shall be awarded to the bidder achieving the **highest combined total score** from both the non-financial and financial evaluations.

6.9. Non-financial evaluation criteria are derived from the requirements set out in Appendix 1 (Terms of Reference). The detailed scoring sub-criteria, as provided in the Excel evaluation sheets, are structured to ensure traceability between ToR requirements and evaluation elements.

After the evaluation of the technical proposal and qualification criteria, candidates who have obtained a minimum of 70 points out of max 100 points will be considered for the financial proposal evaluation. Note, that if the bidder receives less than 30% in any criterion (listed in the tables below), they will not qualify for the further evaluation.

The table below shows the breakdown of technical and qualification criteria for the Real-Time Gross Settlement (RTGS) System.

Evaluation of technical and qualification criteria - Summary of Evaluation Focus	Maximum Score
Bidder's qualification requirements – Proven experience, credibility, and long-term reliability in implementing messaging and payment infrastructure solutions for central banks and financial institutions.	15
Functional requirements - Functional and operational coverage, interoperability, and integration capabilities.	40
Non-Functional requirements - Reliability, performance, and system availability under high-load conditions.	10

Evaluation of technical and qualification criteria - Summary of Evaluation Focus	Maximum Score
Technology & Architecture requirements - Scalability, flexibility, and technical robustness across hybrid and virtualized environments.	10
Security requirements - Cybersecurity governance, access control, compliance with standards, and operational resilience.	15
Implementation approach - Quality and realism of the implementation plan, governance, testing, and risk management.	10
Total Technical Score	**100**

6.10. In this methodology, the Financial Criteria weight is 30%. Accordingly, the maximum number of points assigned to the financial proposal is allocated to the lowest price proposal. All other price proposals receive points in inverse proportion. The formula is as follows:

$P = y (p/z)$

Where:

P = points for the financial proposal being evaluated
y = maximum number of points for the financial proposal
p = NPV of the lowest priced proposal
z = NPV of the proposal being evaluated.

During the price proposal comparison, not only is the offered price evaluated, but also the Net Present Value (NPV) of each proposal, taking into account all expected payments over the duration of the contract. The present value is calculated using the discount rate defined by the Procuring Entity.

6.11. "Bidder's overall impression" is the overall impression of the bidder based on reference checks, site visits, and interactions during the evaluation process. It reflects Purchaser's confidence in the bidder's professionalism, transparency, responsiveness, implementation experience, and ability to act as a reliable long-term partner.

6.12. The Committee shall determine and announce which bidders have been selected and which have not, from among those whose proposals were deemed to meet the requirements of the Invitation. In the event of equal combined scores:

a. simultaneous negotiations shall be conducted with the concerned bidders to achieve a price reduction and determine the selected bidder,

b. the Secretary of the Committee shall simultaneously and electronically notify the concerned bidders of the terms, duration, day, time, and place of the negotiations,

c. based on the prices offered during the negotiations, the selected and non-selected bidders shall be determined and announced. If the combined scores remain equal after negotiations, the preference shall be given to the proposal with lower price.

6.13. If the prices proposed by bidders meeting the requirements of the Invitation exceed the estimated/budgeted cost, the Committee may either declare the procurement procedure invalid or declare the bidder who submitted the lowest price proposal the selected bidder, provided that the rights and obligations of the parties under the contract come into effect only if additional financial resources are allocated and an agreement on that basis.

6.14. If the evaluation of a proposal reveals inconsistencies with the requirements of the Invitation, the Secretary of the Committee shall notify the bidder electronically and offer the opportunity to correct the discrepancy.

6.15. If the bidder corrects the discrepancy within upon agreed time, the proposal shall be considered satisfactory. Otherwise, the proposal shall be deemed insufficient and rejected.

6.16. A Committee member or Secretary shall not participate in the Committee's work if it is revealed that an organization founded by that member or Secretary, or in which they have a share, or a person related to them by close kinship or in-law relationship (parent, spouse, child, sibling, grandparent, or grandchild, as well as spouse's parent, child, sibling, grandparent, or grandchild) or an organization founded or owned by that person, has submitted a proposal. In such as case, the Committee member or Secretary shall immediately withdraw from the procedure.

6.17. After the proposals are opened and finalized, a protocol shall be drawn up according to the established procedure and signed by the Committee present at the session.

6.18. Bidders may request copies of the Committee meeting minutes, which will be provided within 1 (one) working day. Bidders or their representatives may attend the proposal opening and award notification sessions by emailing the Procurement Coordination Service at **procurement@cba.am** at least 1 (one) day in advance, including their name, surname, and organization. Bidders must present an identity document, and representatives must provide a valid power of attorney. Copies of the commission's meeting minutes can be requested and will be provided within one working day.

6.19. The proposals shall be evaluated, and selected bidder determined, per individual Lot.

6.20. If the selected bidder refuses to sign the contract or becomes ineligible to execute it, the next ranked bidder shall be recognized as the selected bidder by decision of the Committee.

6.21. The Committee may verify the authenticity of the information submitted by the bidder through official sources or by obtaining a written opinion from the relevant authorities. In such cases, the relevant state and local self-government bodies shall provide a written conclusion within 2 (two) working days following the receipt of the request. If the submitted information is found to be untrue, the bidder's proposal shall be rejected.

6.22. Before contract execution, the Purchaser shall notify all bidders of the decision regarding contract award no later than the 1 (one) working day following the adoption of the decision on the selected bidder. The decision shall include summary information on the evaluation of proposals, the justification for selecting the winning bidder, and a statement on the inactivity period.

7. BID SECURITY

7.1. The Bidder shall, together with the Proposal, provide a bid security. The amount of the bid security shall be 2 (two) percent of the price proposed in the Proposal for the implementation costs.

7.2. The bid security shall be provided in the form of:

- Cash or;
- a bank guarantee, valid for at least 90 working days starting from the Deadline for Submission of Proposals.

The bid security provided in cash shall be transferred to the Purchaser's account No. 103001702119 (indicating the purpose: "Bid Security – [procedure code]").

For AMD: N 103001702119

For USD: Beneficiary's Bank: JPMorgan Chase Bank, NY
SWIFT code: CHASUS33
Beneficiary: Acc. No:001-1-010782
Central Bank of the Republic of Armenia
SWIFT (BIC) code: CBRAAM22

For EUR: Beneficiary's Bank: Commerzbank, Frankfurt, Germany
SWIFT BIC: COBADEFF
Beneficiary: Acc. No: 400886424101

Central Bank of the Republic of Armenia
SWIFT (BIC) code: CBRA AM 22

7.3. The bid security, in the form of a bank guarantee, should be provided by the Issuing Bank through an authenticated SWIFT message not later than upon agreed deadline to the Advising Bank. The Guarantee should be submitted in paper form upon request. In addition, a scanned copy of the original guarantee may also be provided.

7.4. The bid security shall be returned within 5 (five) working days after the contract is signed. If the procurement procedure is declared unsuccessful, the bid security shall be returned within 5 (five) working days after the expiration of the inactivity period.

In the case of a Bank guarantee, the Purchaser shall release the guarantee through an authenticated SWIFT message within the timeframes specified in this clause regarding the return of the bid security.

The bidder shall pay the bid security (i.e. it shall not be returned) if the bidder:

1) is selected as the winning bidder but refuses or is deprived of the right to execute the contract;

2) violates an obligation undertaken within the framework of the procurement process, resulting in the termination of the bidder's further participation in the process.

In case of Bank Guarantee, the Purchaser shall submit the demand for payment to the Issuing Bank by authenticated SWIFT message within 5 (five) working days following the date on which the basis for the payment of the guarantee arises, but not later than the maturity date of the guarantee.

7.5. Banks use third correspondent banks for sending an authenticated SWIFT message if they haven't RMA Exchange with each other in place. All associated costs related to the issuance, transmission, and confirmation of the guarantee, including any intermediary bank fees, shall be borne by the bidder.

8. CONTRACT PERFORMANCE AND ADVANCE PAYMENT SECURITIES

8.1 Based on the requirement to provide contract performance security, within 20 (twenty) working days from the date of receipt of the relevant notification in the case of bank guarantee and 5 (five) working days in the form of cash, the selected bidder shall provide contract performance security.

8.2 The amount of contract performance security shall be 10 (ten) percent of the implementation costs for the implementation period. The final terms of the security shall be discussed and agreed with the selected bidder. The contract performance security shall be provided in the form of cash or a bank guarantee. The guarantee must be valid at least until the 90th working day following the date of the final acceptance act.

- In the case of a bank guarantee, the contract security shall be submitted in a format approved by the Purchaser prior to contract signature. The contract security, in the form of a bank guarantee, should be provided by the Issuing Bank through an authenticated SWIFT message not later than upon agreed deadline to the Purchaser. The Guarantee should be submitted in paper form upon request. In addition, a scanned copy of the original guarantee may also be provided. Banks use third correspondent banks for sending an authenticated SWIFT message if they haven't RMA Exchange with each other in place. All associated costs related to the issuance, transmission, and confirmation of the guarantee, including any intermediary bank fees, shall be borne by the bidder.
- Contract performance security provided in cash shall be transferred to the Central Bank's bank account (the procedure reference number must be indicated in the "Purpose" field):

  For AMD: N 103001702119

  For USD: Beneficiary's Bank: JPMorgan Chase Bank, NY
  SWIFT code: CHASUS33
  Beneficiary: Acc. No:001-1-010782
  Central Bank of the Republic of Armenia
  SWIFT (BIC) code: CBRAAM22

  For EUR: Beneficiary's Bank: Commerzbank, Frankfurt, Germany
  SWIFT BIC: COBADEFF
  Beneficiary: Acc. No: 400886424101
  Central Bank of the Republic of Armenia
  SWIFT (BIC) code: CBRA AM 22

8.3 A contract shall be signed with the selected bidder if the latter provides the required contract performance security.

8.4 If a contract executed within the framework of a multi-component procurement procedure is terminated due to non-performance or improper performance of any individual component(s), the contract performance security shall be paid only in the amount calculated for the relevant component(s).

8.5 In case of Bank Guarantee, the Purchaser shall submit the demand for payment to the Issuing Bank by authenticated SWIFT message within 5 (five) working days following the date on which the basis for the payment of the guarantee arises, but no later than the maturity date of the guarantee. If the bank rejects the request due to incomplete documentation, the Purchaser shall submit a new request within 2 (two) working days of receiving the rejection.

8.6 The Purchaser shall return the contract performance security as follows:

- In the case of a Bank guarantee, the Purchaser shall release the guarantee through an authenticated SWIFT message within 5 (five) working days following the date on which the basis for return arises,
- In the case of a penalty, the Purchaser shall make a written notification regarding the return of contract performance security to the bidder who provided it, within 5 (five) working days following the date on which the basis for return arises.

8.7 If the contract provides for an advance payment by the Purchaser, the selected bidder shall also provide the Purchaser with advance payment security in the amount of the advance payment, in the form of a bank guarantee, valid at least until the 90th working day following the date of the final acceptance act.

8.8 The Purchaser shall notify the issuing bank in writing regarding the release of the advance payment security within 5 (five) working days following the date of the final acceptance act

8.9 The procedure for repayment of the advance payment is defined by the contract.

8.10 All bank guarantees shall be unconditional and irrevocable issued by a bank agreed with the Purchaser.

9. EXECUTION OF THE CONTRACT

9.1. The contract shall be executed by the Purchaser based on the decision of the Committee.

9.2. The period of inactivity for this procedure shall be 10 (ten) calendar days. The period shall not apply if only one bidder submits a proposal and a contract is executed with that bidder.

9.3. On the fourth working day following the expiration of the period of inactivity defined in clause 9.2 of this Invitation, the Purchaser shall electronically notify the selected bidder by submitting a proposal to execute a contract and the draft contract, which shall include a complete description of the product and services as set forth in the selected bidder's proposal. The contract may not be executed earlier than the fourth working day following the expiration of the inactivity period specified in clause 9.2 of this Invitation.

9.4. If, after receiving the notice of award and draft contract, the selected bidder does not approve the contract and submit the contract performance security to the Purchaser within the period stipulated in clauses 8.1 and 8.2 of this Invitation, the bidder shall be deprived of the right to sign the contract. The draft contract approved by the selected bidder shall be submitted to the Purchaser in writing.

9.5. Before the expiration of the period provided for in clause 9.4 of this Invitation, the parties may agree to make changes to the draft contract. Such changes shall not involve any material modifications to the description of the subject of the procurement, nor shall they result in an increase in the advance payment or the price proposed by the selected bidder.

9.6. The Purchaser shall execute the contract if no bidder appeals the decision to execute the contract within the inactivity period defined in this Part. The contract shall be deemed invalid if executed before the expiration of the inactivity period, without properly executing the contract, or following a notice declaring the procurement procedure to be invalid.

10. DECLARING THE PROCEDURE INVALID

10.1. The Committee shall declare the procedure invalid if:

- no proposals are submitted,
- none of the proposals meets the requirements of the Invitation,
- the procurement needs cease to exist,
- no contract is executed.

10.2. The Purchaser shall notify all bidders participating in the tender of the reasons for declaring the procurement procedure invalid.

11. BIDDERS' APPEAL RIGHTS

11.1. All interested persons have the right to appeal the actions (or inactions) and decisions of the Purchaser and the Committee in accordance with the procedure established by the Civil Procedure Code of the Republic of Armenia (hereinafter referred to as the "Code").

11.2. All persons have the right to appeal the descriptions of the subject of procurement or the requirements of the Invitation prior to the proposal submission deadline, in accordance with the procedure established by the Code.

11.3. Relations related to this procedure are not administrative in nature and shall be governed by the laws of the Republic of Armenia regulating civil law relations.

Appendix 1

Tender Invitation
Reference Number: CBA-2025-064

TERMS OF REFERENCE

LOT	Name	Technical Description	Unit of Measurement	Quantity
1.	Acquisition of Real-Time Gross Settlement (RTGS) system for the Needs of the Central Bank of the Republic of Armenia.	The technical specification is presented in detail in Terms of Reference and applies together with the General Terms & Conditions stated below	Lot	1

RTGS Terms of Reference

1 Executive Summary 23
1.1 What is Being Procured 23
1.2 What is the Objective 24
1.3 Impact 24
1.4 Expected Outcome 24
2 Introduction 25
2.1 Purpose of this RFP 25
2.2 About Armenia Financial Sector 25
2.3 About the Central Bank 26
2.4 Overview of the Functions of the Central Bank 26
2.5 Operational Status of the Central Bank 27
2.6 Objective of the Project 28
2.7 Project Stakeholders 29
3 Scope of Work 31
3.1 Scope of Requirements 31
3.2 Adaptation to Local Regulatory, and Language Requirements 31
3.3 Multi-Year Support and Co-Development Partnerships 31
3.4 Licensing Model and Flexibility 31
3.5 Project Site 31
3.6 Structured Response Template for Bidders 32
3.7 Technical Components 32
3.8 Payment Engine and Core Banking System Interaction 34
4 Core Banking and Payment Engine Interaction Models Description 35
Interaction Models 35
4.1 Model I 35
4.2 Model 2 37
5 Functional Requirements 40
5.1 Payment Engine Functional Capabilities 40
5.2 Integration Functional Requirements 57
6 Non-Functional Requirements 60
6.1 Performance & Reliability 60

6.2 Resilience & Availability 61
7 Technology & Architecture Requirements 62
7.1 Hardware Layer 62
7.2 Infrastructure Layer 62
7.3 Platform Layer 63
7.4 Application Layer 64
8 Security Requirements 66
8.1 Operational Security 66
8.2 Cybersecurity & Resilience 68
9 Qualification and Other Relevant Requirements 71
9.1 General Eligibility Criteria 71
9.2 Bidder's Qualification Criteria 71
9.3 Account Management and Project Team Qualification Requirements 72
9.4 Financial Standing 72
9.5 Cost & Licensing 73
9.6 Source Code Escrow Requirements 74
10 Implementation / Delivery 75
10.1 Proposed Implementation Roadmap 75
10.2 Implementation & Support 76
11 Deliverables 78
11.1 Expected Deliverables and Planned Timelines 78
11.2 Project Documentation 78
11.3 Acceptance Criteria 81
12 Appendix 82
12.1 Acronyms 82
12.2 Definitions 86
General Terms & Conditions (T&Cs) 89
T&Cs of Payments and delivery models 92
T&Cs of Implementation Roadmap. 94
T&Cs of Penalty Calculations. 94
T&Cs of Project management Governance 94
T&Cs of Support and Maintenance 95

1 Executive Summary

In light of the economic growth over recent years, the Central Bank of Armenia launched an initiative in 2024 to renew its Financial Market Infrastructure, including existing Financial Messaging System and Real-Time Gross Settlement solution. In a broader sense, the initiative includes the implementation of the following key systems:

- Financial Message Exchange System: An application-level platform for secure financial messaging that connects market participants to the CBA payment infrastructure through CBANet (the CBA interbank network).
- Central Bank Gateway System: a centralized platform within the Central Bank integrating external (Messaging Hub, SWIFT, etc.) and internal systems (Core Banking, Monetary Policy Instruments System, GSASS, RTGS etc.).
- Payment Engine: The new RTGS system serving as the core processing and settlement infrastructure for interbank payment transactions.

The current infrastructure components are reaching the end of their lifecycle, and the existing RTGS solution no longer meets modern business requirements in terms of functionality, scalability and resilience. For this reason, the CBA is seeking to replace its existing RTGS solution.

1.1 What is Being Procured

The CBA is procuring a new RTGS system as a cornerstone of its national financial market infrastructure modernization program. The CBA is aiming to have secure, highly resilient, interoperable, and future-ready central bank RTGS system that provides safe real-time settlement in central bank money while supporting wider access and ISO 20022 data richness.

The solution must incorporate advanced operational capabilities, including disaster recovery, high availability, and real-time monitoring, and will integrate seamlessly with the CBA's broader architecture, including the Central Bank Gateway System, Control Centre, and Central Data Store.

For consistency, this document uses the term 'Payment Engine' to refer to the technical platform or solution being procured. The Payment Engine will deliver and support the Central Bank's RTGS operations and related payment processing capabilities. References to the 'RTGS' in this document denote the functional aspect of real-time settlement, whereas 'Payment Engine' refers to the system implementing that functionality.

This procurement excludes the Messaging Service (consisting of Financial Message Exchange System and Central Bank Gateway System), which was addressed under a separate RFP published in 09.12.2025 (Procedure reference number CBA-2025-064).

1.2 What is the Objective

The new RTGS system is a strategic enabler of Armenia's financial market modernization, designed to:

- Strengthen resilience, security, and operational continuity in the national payment ecosystem.
- Align with international standards, including ISO 20022 and the BIS Principles for Financial Market Infrastructures (PFMI).
- Reduce settlement and operational risk.
- Improve operational efficiency and transparency for the CBA and market participants, while offering a broader range of services to support effective payment and liquidity management, as well as enhanced monitoring and reporting capabilities.
- Enable greater interoperability with domestic, cross-border, and regional payment systems and other financial market infrastructures (FMIs).
- Strengthen cybersecurity and operational resilience.

1.3 Impact

The successful implementation of the RTGS system will:

- Establish a secure, modern, and future-ready settlement system for Armenia's financial sector;
- Reduce settlement risk and strengthen overall payment system resilience;
- Enhance the efficiency and reliability of high-value, time-critical payments; and
- Support the CBA's broader financial infrastructure modernization strategy.

1.4 Expected Outcome

The RFP is expected to result in comprehensive vendor responses that enable CBA to assess, validate, and compare proposed RTGS solutions. Vendor submissions should address all relevant sections of this RFP and provide:

- A clear solution architecture and integration strategy;
- Detailed plans for delivery, configuration, deployment, testing, training, and knowledge transfer plans;
- Proposals for post–go-live support and maintenance, including clear SLAs, disaster recovery, and business continuity measures;
- A transparent commercial offer with itemized costs for software, services, licenses, training, and long-term support, and any required localization or customization;
- Mechanisms such as escrow agreements to safeguard continuity in the event of vendor discontinuation.

2 Introduction

2.1 Purpose of this RFP

The purpose of this Request for Proposal (RFP) is to invite qualified vendors and solution providers to submit comprehensive proposals for the modernization of Armenia's national financial market infrastructure. This modernization will include the renewal of the Real Time Gross Settlement (RTGS) system.

Through this RFP, the Central Bank of Armenia seeks to engage experienced, capable, and innovative firms with a strong track record in implementing ISO 20022-compliant RTGS and high-value payment infrastructures, and delivering secure, resilient, and scalable architectures designed for mission-critical financial systems.

2.2 About Armenia Financial Sector

As of July 2025[1], Armenia's financial system is composed primarily of 17 commercial banks, 9 insurance companies, 16 Payment Service Providers, 43 credit organizations and 23 investment companies. The banking sector continues to dominate the financial landscape, with total assets reaching AMD 11 trillion (approximately USD 28 billion), marking an annual increase of around 13%. This growth is driven by robust economic performance, digital financial service adoption, and the continued expansion of trade and services.

At the same time, total bank loans reached AMD 7.1 trillion (approximately USD 18 billion) and deposits amounted to AMD 6.7 trillion (approximately USD 17 billion) reflecting growing public trust, improved financial literacy, and enhanced digital banking outreach. The capital adequacy ratio across banks remains well above regulatory thresholds, indicating a strong and stable banking environment.

The CBA remains the primary regulator, and supervisor of the financial sector (commercial banks, insurance, securities, credit organizations, and payment systems) and is also responsible for overseeing critical financial market infrastructures. Regulatory reforms and ongoing digital transformation initiatives such as e-wallet integration, real-time payments, and modernization of banking services, have significantly improved financial inclusion. Local payment infrastructures such as Armenia Card (ArCa), which handles card and instant payment processing, play a central role in Armenia's financial ecosystem. Alongside this, the activity of Payment Service Providers contributes to an increasingly dynamic fintech and payments landscape.

Non-bank financial institutions (NBFIs) especially in microfinance and SME lending continue to play a vital role, particularly in underserved rural areas.

[1] https://www.cba.am/en

Despite ongoing regional geopolitical tensions and external economic uncertainties, Armenia has maintained macroeconomic and financial stability, supported by prudent monetary policy, resilient supervision, and an effective deposit insurance system. This has helped reinforce systemic trust and reduce financial sector vulnerabilities.

Armenia's stable, diversified, and increasingly inclusive financial system remains a core enabler of sustainable economic development, particularly as the country accelerates digitalization and regional economic integration.

2.3 About the Central Bank

The Central Bank of Armenia (CBA) is an independent public institution tasked with ensuring price and financial stability in the Republic of Armenia (RA). Established in 1993 following Armenia's independence, the CBA operates under the Law on the Central Bank and is governed by its Board, which is responsible for setting strategic direction and approving monetary and financial stability policies.

The CBA is headquartered in Yerevan and plays a central role in formulating Armenia's financial and economic policy framework. Its independence is constitutionally guaranteed, ensuring that its decisions are free from political interference and focused on long-term economic and financial stability.

In addition to its core regulatory functions, the Central Bank acts as the government's fiscal agent, managing public debt instruments and servicing state payments. The CBA also fosters innovation in the financial sector, promotes financial inclusion, and drives digitization efforts across the Armenian economy. It has taken a proactive role in advancing Armenia's fintech landscape and enhancing the resiliency of national financial infrastructures.

The Central Bank actively engages with regional and international organizations, and participates in cross-border regulatory dialogues and cooperative frameworks.

2.4 Overview of the Functions of the Central Bank

The Central Bank of Armenia (CBA) has a broad and evolving mandate consistent with the principles of modern central banking. Its principal functions include:

- Monetary Policy: Formulates and implements monetary policy to maintain price stability, using tools such as interest rates and reserve requirements.
- Currency Issuance and Management: Sole issuer of the Armenian dram (AMD), responsible for ensuring adequate and secure currency supply and combating counterfeiting.

- Financial System Supervision and Regulation: Licenses and supervises banks, credit organizations, insurance firms, securities market participants, non-bank payment service providers, and investment firms.
- Payment System Oversight and Operation: Operates and oversees critical payment and settlement infrastructures, including the current RTGS system, to support safe, efficient, and reliable interbank payments.
- Government Fiscal Agent Functions: Acts as the banker and fiscal agent for the Armenian government, including management of the domestic debt market and execution of government payments.
- Reserve Management: Manages Armenia's official reserves and intervenes in the foreign exchange market when necessary to maintain market order and exchange rate stability.
- Financial Stability Monitoring and Macroprudential Policy: Conducts stress testing, systemic risk analysis, and macroprudential surveillance to pre-empt and mitigate threats to financial stability.
- Financial Innovation and Inclusion: Supports the development of digital finance, open banking, and alternative delivery channels, especially to underserved regions and populations.
- Consumer Protection and Financial Education: Promotes transparency and fairness in financial services, ensuring customer rights are protected, and leads public education initiatives on financial literacy.

2.5 Operational Status of the Central Bank

The Central Bank of Armenia operates in a stable, institutionalized, and technologically progressive environment, supported by a set of national financial infrastructures that it directly manages. Its systems are technologically mature but remain under active modernization to align with international standards. Armenia's payment infrastructure is built on a domestic (non-SWIFT) CBA interbank proprietary network (CBANet), relying on BankMail as the secure messaging platform and the CBA's Core Banking system. The latter is a monolithic platform that performs core banking, RTGS as well as general ledger functionalities. The payment infrastructure relies on a local message format (AM-HT[2]) for interbank payment and securities transactions. Together these components provide a strong infrastructure for wholesale and retail settlement.

The CBA currently:

- Operates the Electronic Payment System (EPS/RTGS), which supports real time settlement of wholesale and retail interbank payments in central bank money. However, the current solution requires enhancements to incorporate advanced capabilities such as ISO 20022 messaging, liquidity-saving mechanisms, and improved cyber-resilience.
- Oversees the Central Depository of Armenia (CDA), which is the central depository and Securities Settlement System (SSS) for non-government securities issued in Armenia and provides safekeeping, central register, clearing and settlement services to its participants.

[2] Messaging format which is currently used in Armenia (see ***Error! Reference source not found.***)

- Acts as the central depository for RA government securities, for which it operates Government Securities Accounting and Settlement System (GSASS), that provides safekeeping, central register, clearing and settlement services to its participants.
- Supervises ancillary payment systems, including instant payments, card-based ArCa system and the STAK remittance system, in which the settlements are executed in EPS/RTGS, based on multilateral net positions.

The CBA's operational strategy emphasizes automation, efficiency, and real-time capabilities across its functions. It has implemented an integrated internal accounting system and is pursuing initiatives to improve internal data analytics, cross-system interoperability, and policy decision support.

In terms of human capital and institutional capacity, the CBA employs highly qualified professionals across banking supervision, economic research, financial operations, IT, and cybersecurity. The Central Bank maintains strong international cooperation channels and draws on global expertise and benchmarks in its ongoing reform agenda.

In preparation for the modernization of the national payment system, the CBA has already undertaken a comprehensive assessment of its EPS/RTGS and Messaging infrastructures via an extensive gap assessment and requirements elicitation exercise, including looking into legal framework, business processes, and future interoperability requirements with retail, cross-border, and digital currency solutions.

2.6 Objective of the Project

The CBA is undertaking a comprehensive modernization of its national financial market infrastructure, with a focus on implementing a new RTGS system. This strategic initiative aims to enhance the efficiency, security, and resilience of Armenia's financial ecosystem, while ensuring alignment with international standards and future-proofing the country's critical financial market infrastructures.

Key Components of the Modernization:

The Payment Engine will facilitate interbank payments in real time, support payment and queue prioritization, advanced liquidity management, and other RTGS-specific functionalities, and strengthen monitoring and reporting capabilities for both the CBA and market participants. Replacing the legacy platform - operational since the early 2000s and constrained by monolithic architecture within Core Banking System - the new Payment Engine will feature modular design. The new system will support high availability, robust reporting and analytical functions, complemented by modern, user-friendly interfaces, dashboards, online portals for administrators, users and market participants with native support for ISO 20022 messaging standards.

Strategic Goals:

- Ensure high levels of system availability, performance, and security for critical payment services.

- Align with international best practices and standards, including ISO 20022, the BIS Principles for Financial Market Infrastructures (PFMI).
- Enhance operational resilience through robust business continuity, disaster recovery, and cybersecurity capabilities.
- Improve liquidity and queue management, payment prioritization, and automation to support efficient settlements.
- Enable interoperability with CBA internal systems and with domestic, regional, and cross-border payment infrastructures.
- Provide a scalable foundation for future capabilities such as instant payments, advanced regulatory reporting, Central Bank Digital Currency (CBDC), and regional integration.
- Strengthen transparency, trust, and systemic stability within Armenia's financial ecosystem.

Implementation Approach:

The project will be executed under a unified, structured implementation framework covering all phases from planning and development to testing, deployment, and transition to steady state. Interoperability, seamless integration with existing and future systems, and long-term extensibility will be key evaluation criteria. Preference will be given to proven, configurable solutions or customized implementations of existing solutions over entirely bespoke developments to reduce delivery risk and ensure faster time to market.

For smooth implementation of the project, it is essential that the RTGS vendor has full visibility of all moving parts and involved stakeholders. The solution provider should be aware that several interconnected projects will be running in parallel during the implementation phase. These include the implementation of the Messaging Service and multiple related projects. At the same time, the migration from AM-HT to ISO 20022-AM standard will be underway. In the Financial Market Infrastructure modernization journey the CBA has adopted the staged transition approach. Therefore, changes will be introduced sequentially, one at a time.

2.7 Project Stakeholders

The success of this modernization depends on effective coordination among a diverse group of internal and external stakeholders. Bidders are expected to operate in a collaborative environment and align with the roles and responsibilities of all parties involved.

Internally, key stakeholders include senior management, the Steering Committee, and departments responsible for Payment Services, IT, Information Security and Cybersecurity, Finance, Compliance and Regulation.

Externally, the project engages commercial banks, financial institutions, the Ministry of Finance, the Central Depository of Armenia, and various technology vendors and integration partners who contribute to system implementation, testing, and interoperability.

Bidders shall to consider how their proposed solutions and delivery approaches will support effective engagement across this multi-stakeholder environment. Experience managing complex, cross-functional delivery in regulated financial ecosystems will be a key evaluation factor in subsequent phases.

3 Scope of Work

3.1 Scope of Requirements

The requirements outlined in this RFP are intended to represent the minimum scope of services expected from bidders. CBA reserves the right to request additional features, or enhancements that may arise during discussions, implementation, or operation.

Any such additional requirements will be subject to mutual agreement between the CBA and the selected vendor(s), including scope, timelines and associated pricing. This provision is not intended to create an open-ended obligation, but rather to ensure that the proposed solution remains adaptable to evolving needs and regulatory expectations.

If bidders fail to address certain requirements entirely or provide responses that are incomplete or not aligned with the stated expectations, the CBA will follow up on those items, particularly on requirements deemed critical to the assessment.

3.2 Adaptation to Local Regulatory, and Language Requirements

The Bidders must demonstrate the capability of the proposed solution to be localized in full compliance with local regulatory, reporting, and language requirements. Bidders shall provide documented examples of previous implementations where business rules, validation logic, and user interfaces were adapted to meet local market practices and regulatory obligations.

3.3 Multi-Year Support and Co-Development Partnerships

The Bidders must offer multi-year support agreements covering a minimum of 10 years from system acceptance, including defined SLAs and performance guarantees. The proposal must demonstrate an aligned product roadmap that supports the Central Bank's long-term objectives and provide structured opportunities for co-development and joint innovation throughout the support period. The Central Bank reserves the right to negotiate additions, deletions, or modifications to the multi-year support terms and SLA submitted by Bidders.

3.4 Licensing Model and Flexibility

Bidders must explain the licensing model used for the Payment Engine.

3.5 Project Site

The place of supply and implementation of the system is the Central Bank of the Republic of Armenia, located at 6 Vazgen Sargsyan Street, Yerevan, 0010, Republic of Armenia.

The System (the Payment Engine) must be deployed within the internal infrastructure (on-premises) of the Central Bank (cloud-based solutions are not acceptable).

3.6 Structured Response Template for Bidders

To support a fair, consistent, and efficient evaluation process, bidders are kindly requested to structure their proposals using the response document templates provided with this RFP. The templates are intended to provide clarity on what information the CBA seeks to gather at this stage of the procurement process.

3.7 Technical Components

3.7.1 Conceptual View

To seamlessly migrate Central Bank's various services to a modern, modular architecture, the new platform shall be built on pluggable services. This approach enables incremental upgrades and ensures that new services or instruments such as tokenized assets can be added at any time without major architectural changes.

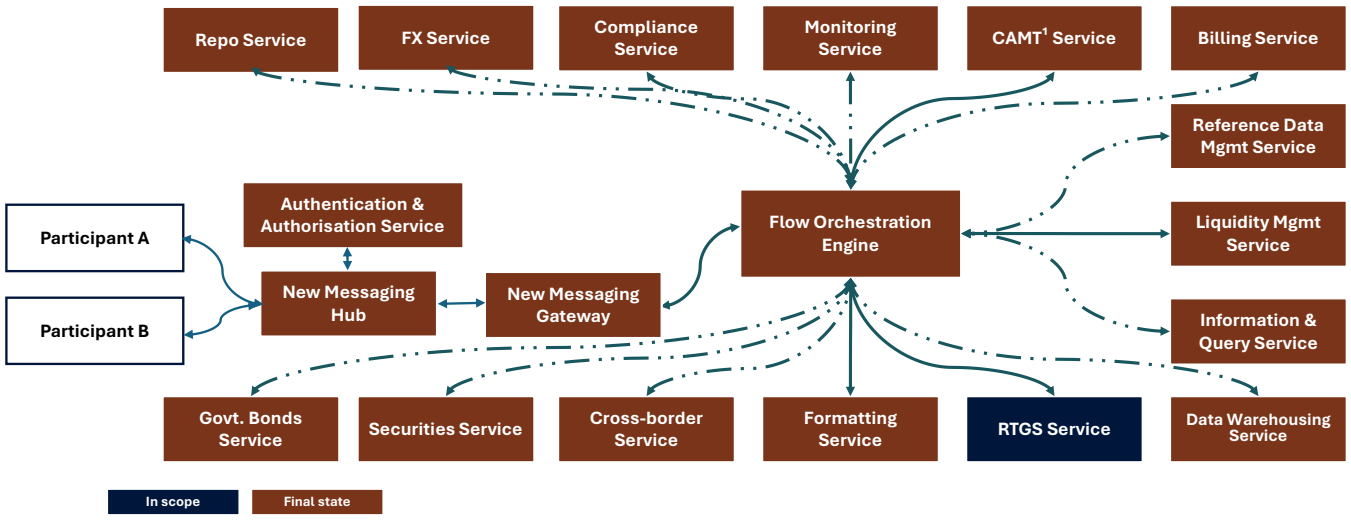


Figure 1: Business view on the financial market infrastructure

In scope of this RFP is: Payment Engine which provides RTGS Service

3.7.2 Logical View

Error! Reference source not found. provides a logical view of the components that make up the platform.

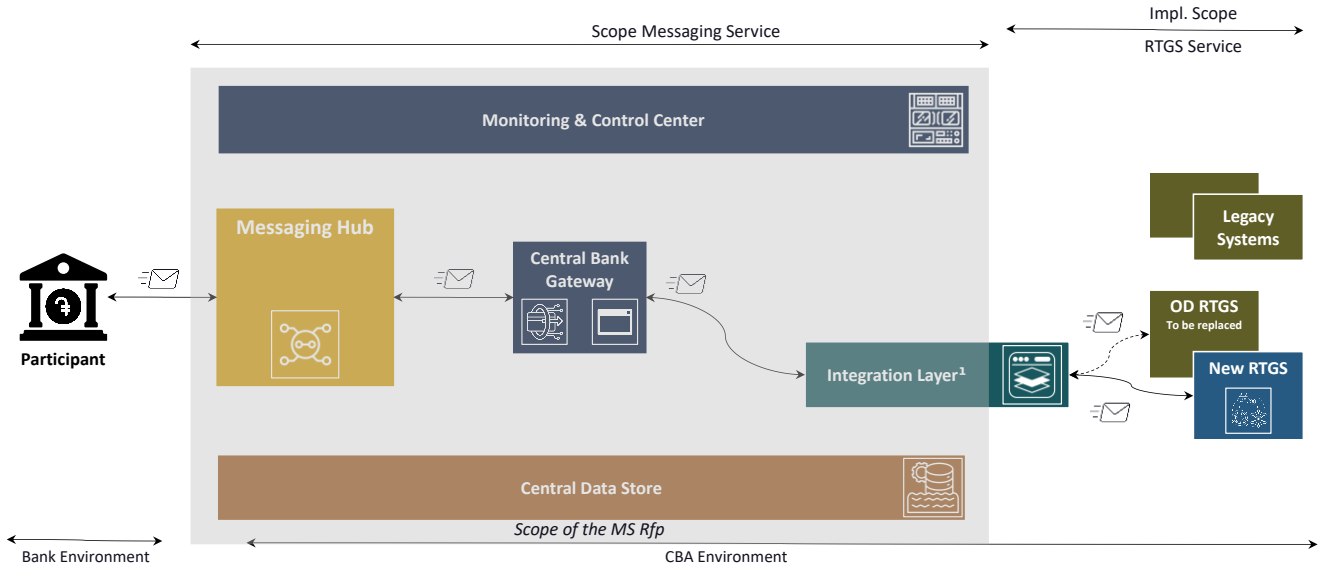


Figure 2 Logical view

At a later stage support for monitoring and control, represented as "Monitoring & Control Center" in ***Error! Reference source not found.*** *3* can either be one integrated component within CBA's Market Infrastructure or through the vendor-provided plugins. The Monitoring & Control Center will be part of CBA's Web Portal, which will provide functionality to CBA internal staff but also to the market participants. The CBA Web Portal is not in scope of this RFP.

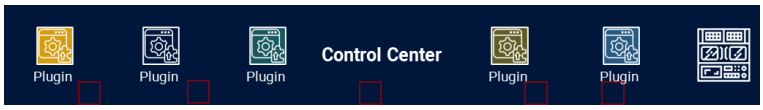


Figure 3 Monitoring & Control Centre on the basis of plugins

The Central Data Store will be either designed as a single consolidated data repository or implemented as an integrated environment combining multiple component-specific databases, as shown in *4*. This flexible approach allows vendors to integrate their respective data stores into the Central Data Store while maintaining a unified data architecture.



Figure 4: Central Data Store integrating component specific databases

Note that bidders **are not asked** to provide a commercial offering for the Monitoring & Control Center or the Central Data Store. Purpose of the information given above is to provide bidders with the end-to-end context.

3.7.3 Business Capabilities

The **Payment Engine** will receive, process and send payment instructions in real time, updating the balances of the accounts involved, either determined as defaults based on the debtor and creditor agents or based on the accounts mentioned in the instruction itself. The system will perform both technical and business validations. Technical validation will ensure that inbound messages or files comply with the defined schema, verifying syntax, format, structure, and mandatory fields, as well as message headers and wrappers. Business validation will ensure that the content of each message is correct for further processing, validating business data against defined business rules for the message and its usage. The Payment Engine will also support queuing, gridlock resolution, and advanced liquidity management mechanisms to optimize settlement efficiency, as well as provide enhanced analytical, monitoring, and reporting capabilities for the CBA and market participants.

3.8 Payment Engine and Core Banking System Interaction

The CBA's current EPS/RTGS operates as a monolithic platform closely embedded within the CBA's Core Banking System. As part of the RTGS modernization project, it is essential to separate the RTGS and Core Banking functionalities to achieve greater modularity, scalability and operational independence.

The interaction between the two systems will therefore be based on well-defined integration models that ensure seamless data exchange, consistent accounting, and synchronized settlement.

4 Core Banking and Payment Engine Interaction Models Description

Interaction Models

The CBA has defined two potential models for the interaction between the new Payment Engine and the Core Banking System. These models differ in where the settlement occurs and account entries are maintained, how liquidity is managed, and how integration between the Payment Engine and Core Banking is performed.

The two models, Model I (Core Banking Accounting), and Model II (RTGS Accounting), represent alternative architectural and operational approaches that balance real time settlement efficiency, integration complexity, and operational resilience.

In Model I, the Core Banking System remains the system of record for all participant account balances and settlement postings, while the Payment Engine performs orchestration, validation, queuing, and prioritization. Settlement is executed in real time through the Core Banking System.

In Model II, the Payment Engine maintains participant settlement accounts internally and executes settlement postings directly within its ledger. The Core Banking System continues to hold participants' main accounts and liquidity sources, with synchronization between the two systems to ensure consistency and accurate reflection of balances.

The final selection of the operating model will be made during the solution design phase based on

- The capabilities and flexibility of the proposed RTGS solution;
- The financial, operational, and risk management implications of each model;
- The alignment with CBA's long-term architectural and resilience objectives.

Detailed descriptions of each model are provided below.

4.1 Model I

Model I is based on real-time interaction between the Payment Engine and the Central Bank's Core Banking (General Ledger) system. In this model, all account balances are maintained within the Core Banking environment, while the Payment Engine performs orchestration, validation, and queue management for settlement instructions.

Definition of the model

- **Account structure**: Participant's main account is held entirely in the Core Banking (General Ledger) system; the Payment Engine does not maintain internal account balances.

- **Payment Engine functionality**: The Payment Engine receives payment messages, performs both technical and business validations, and manages payment scheduling including future-dated or

timed payments, queuing, and prioritization. It sends requests to the Core Banking system for account validation, funds checking, and settlement posting, receives the corresponding responses, updates payment statuses, and generates outbound messages (e.g. settlement confirmations, rejection notifications, etc.).

- **Core Banking functionality**: The Core Banking system executes account validation, applies priority-based funds checks, performs the actual settlement postings for each RTGS payment, produces account statements, and manages any applicable restrictions. It responds to the Payment Engine with the result of the validation, funds checking, and posting operations to enable payment status updates and subsequent message generation.

- **Payment Engine Settlement request scheduling**: Settlement requests initiated by the Payment Engine to the Core Banking System (for account validation, funds checking, and posting) are automatically repeated based on configurable intervals, frequency, and attempt limits. Payments that cannot be settled due to insufficient funds are placed in a queue and retained until liquidity becomes available or until end-of-day cut-off rules apply.

- **Payment Priorities**: The Payment Engine must support three payment priority levels:

  - HVP for financial-market operations of payments exceeding a defined threshold;

  - URGP for urgent commercial payments;

  - SSTD for standard low-value or lower-priority payments.

- **Reservation and Liquidity Usage**: Two liquidity-reservation types must be supported for HVP and URGP payments, in addition to reservation levels for ancillary systems (e.g. ArCa and STAK). These reservations are maintained on participants' main accounts within the Core Banking system, with reserved amounts automatically adjusted as transactions are settled.

HVP payments use available liquidity within HVP reserve plus the free balance (current balance minus all reservations) and the URGP balance. URGP payments use the URGP reserve plus free balance. SSTD payments use the free balance only. Ancillary systems settlements use their corresponding reserved balances.

- **Reservation Updates**: Liquidity and exposure levels must be configurable and adjustable both at the start of the business day and during intraday operations, following defined Central Bank rules.

- **Non-RTGS Primary Operations**: Funds transfers for Monetary Policy operations, Government Securities Accounting and Settlement System operations cash legs, cash operations, and other transactions not processed via current EPS/RTGS system continue to be processed in the Core Banking system using balances of main accounts. If insufficient funds exist, such operations are rejected or retried according to current rules.

4.2 Model 2

In the Model II the Payment Engine maintains participant settlement accounts internally, and performs settlement postings directly within its ledger with rule-based synchronization to the Core Banking system. The Central Bank's Core Banking (General Ledger) system maintains participants' main accounts.

Definition of the model

- **Account structure**: each participant has a settlement account maintained within the Payment Engine. These accounts cannot have negative balances. The Central Bank also maintains its own RTGS settlement account, which may operate with a negative balance subject to defined limits.
- **Main accounts:** Participants' main accounts remain in the Core Banking (General Ledger) system, where credit lines are defined and managed.
- **Start of Day Liquidity Transfer:** At the start of each operational day, liquidity designated for RTGS settlements is transferred from a participant's main account in the Core Banking system to its corresponding settlement account in the Payment Engine. The Central Bank's settlement account in the Payment Engine starts each day with a zero balance.
- **Intraday Liquidity Movements:** During the business day, liquidity may be transferred between participant's main and settlement accounts in both directions, subject to reservation rules defined in the Payment Engine. Such transfers can be initiated by participants or generated automatically based on predefined conditions or requested by either the Core Banking System or the Payment Engine as part of the liquidity management processes.
- **End of Day Liquidity Repatriation:** At the end of business day, the remaining liquidity, is transferred back to the participant's main account in the Core Banking system. This process ensures the final liquidity position is accurately reflected on the participant's ledger account.
- **Accounting Structure for Liquidity Transfers**: To ensure accurate and synchronized accounting of liquidity movements between the RTGS and the Core Banking system, corresponding transit and mirror accounts are maintained in both environments: The Core Banking system maintains an RTGS Transit Account that records the total liquidity transferred to participants' settlement accounts and is used for ledger postings. The Payment Engine maintains a mirror transit account reflecting the same liquidity movements for reconciliation and reporting. For Central Bank operations, a dedicated Central Bank RTGS Transit Account exists in the Core Banking System, mirrored by a corresponding Central Bank Settlement Account in the Payment Engine.
- **Payment Settlement**: All payments between RTGS participants, including the Central Bank, are settled on the Payment Engine ledger on participants' RTGS settlement accounts according to reservation and prioritization rules. Settlement within RTGS is final and unconditional. Upon completion of each settlement, the system shall generate and transmit the corresponding outbound messages, such as settlement confirmations, debit/credit notifications, etc..
- **Payment Priorities**: the Payment Engine must support three payment priority levels:

  - HVP for financial market operations or payments above a defined threshold;
  - URGP for urgent commercial payments;
  - SSTD for standard low value or lower priority payments

- **Reservation and Liquidity Usage**: Two reservation types must be supported for HVP and URGP payments in addition to several reservation levels for ancillary systems (e.g. ArCa, ArCa Pay and STAK). All reservations are maintained within the Payment Engine on participants' settlement accounts. The reserved amounts are dynamically adjusted as transactions are settled.

HVP payments use available liquidity within HVP reserve plus the free balance (current balance minus all reservations) and the URGP balance. URGP payments use the URGP reserve plus free balance. SSTD payments use the free balance only. Ancillary systems settlements use their corresponding reserved balances, with the RTGS supporting definition, adjustment, and release of these reservations through standardized ISO 20022 messages or equivalent interfaces.

- **Reservation Updates**: Liquidity reservation parameters must be configurable and adjustable both at Start-of-Day and throughout the business day, either according to predefined rules or through standardized ISO 20022 messages or equivalent interfaces. Unlike HVP and URGP reservations, which reset at the end of the day, AS system reservations must be retained overnight.
- **Central Bank Operations**: For Central Bank or its clients' transactions the following rule will apply: If the Central Bank is the debtor, the transaction is initiated in the Core Banking system and sent to the Payment Engine for settlement. If the Central Bank is the creditor, the transaction is settled directly in the Payment Engine as a regular interbank payment.
- **Non-RTGS Primary Operations**: Funds transfers for Monetary Policy operations, Government Securities Accounting and Settlement System cash legs, cash operations, and other transactions not processed via current EPS/RTGS system continue to be processed in the Core Banking system using balances of main accounts. If insufficient funds exist, such operations are rejected or retried according to current rules. If extra liquidity is needed, participant could initiate liquidity transfer from settlement account to main account. Where applicable, Core Banking-primary operations may have assigned priorities that trigger automatic liquidity transfers from RTGS settlement accounts to main accounts under predefined liquidity usage rules.
- **Postings of the settled transactions in the Core Banking System**: Posting of the transactions settled in Payment Engine on the Participant's main account in the Core Banking System could be done by one of the following ways: real time, at the defined intervals, or at the end of the business day (on gross or net basis).
- **Account Statements**: Two statements must be produced daily: one for the main account created by the Core Banking System and one for the settlement account created by the Payment Engine. It should also be possible to generate a combined statement that includes the main account's start-of-day and end-of-day balances along with all payment transactions settled both in the Core Banking System and the Payment Engine.

- **24/7 support**: The Payment Engine must support 24/7 operations with distinct processing capabilities for 'day' and 'night' cycles, independently from the operating hours of the Core Banking system.

5 Functional Requirements

5.1 Payment Engine Functional Capabilities

5.1.1 Settlement & Liquidity

Real-Time Gross Settlement (RTGS) Capability
The proposed solution must support true real-time gross settlement, meaning each transaction is processed and settled individually and immediately, without batching or deferred processing. In the context of Model I, this entails the Payment Engine initiating real-time settlement requests to the Core Banking System for account validation, funds checking, and posting. Under Model II, settlement is executed directly within the Payment Engine through an internal settlement account ledger that records and reconciles all debits and credits (please refer to Chapter 4 Core Banking and Payment Engine Interaction Models Description). Bidders should clearly describe the architectural approach that enables this functionality and highlight any operational limitations or scenarios in which real-time settlement may be impacted, including peak load conditions, message processing or file-based inputs.

Transaction Finality and Irrevocability
Transactions processed by the system must be irrevocable and final immediately upon execution. Bidders shall explain how this is achieved, describing the controls that prevent any alteration or reversal of settlement entries, and the mechanisms that ensure data integrity and real-time confirmation. If the solution maintains an internal settlement ledger (under Model II), it shall demonstrate how immutability and controlled recovery are implemented while maintaining compliance with settlement finality principles.

Duplicate Payment Validation
The Payment Engine must include business-level validation mechanisms to detect and prevent duplicate payment instructions from being processed. Apart from message identifiers, duplicate detection must be based on transaction data elements such as payment reference, amount, value date, debtor, and creditor information. Bidders shall describe the duplicate detection logic, including criteria, error handling, and user notifications, and explain how these controls interact with queuing and settlement processes. Bidders shall also clarify whether duplicate checks are performed as part of the technical validation (e.g. schema, syntax, and mandatory fields) or within a separate business validation layer and confirm how structural and schema validations are handled in the system.

Business Validation
The solution must enforce comprehensive business validations on all payment orders, including participant authorization, payment type consistency, and adherence to defined processing rules. Validations must apply across all input channels and ensure that all message fields, references, and attributes comply with the requirements for each payment type (e.g. interbank transfer, customer payment). The Payment Engine must perform business validation to the maximum extent possible to identify and report all detectable errors within a single validation cycle. Business validation shall include, at a minimum, checks for participant eligibility, account status, duplicate instructions, value

limits, message completeness, and alignment with business rules. Bidders must describe all possible business rules that can be implemented, how these rules are defined, maintained, and enforced, whether validation logic can be configured by the Central Bank without vendor support, and how validation errors are reported to participants.

Credit and Direct Debit Transfer Orders

The Payment Engine must support the full processing of credit transfer and direct debit payment orders in compliance with ISO 20022 standards. It shall validate, queue, and settle both transaction types according to their respective business rules, ensuring correct identification of debtor and creditor roles, mandate validation for direct debits, and adherence to applicable cut-off and settlement timelines. The system shall allow configuration of distinct processing parameters, reservations, and prioritization rules for credit and debit transactions while maintaining consistent validation, posting, and reporting procedures across all payment types.

Field and Reference Data Validation

The Payment Engine must validate message fields and reference data for all transactions. The system must prevent the settlement of incomplete or invalid messages. Bidders must outline validation criteria, reference data management processes, and integration with external data sources where applicable.

Account Validation and Funds Checking Services

The Payment Engine must provide services to validate debtor and creditor account status and to check available balances in real time. The system must also verify time constraints, ensuring that future-dated or timed payments are eligible for settlement based on the effective date and time specified in the payment order. Under Model I, account reference data and balances are maintained in the Core Banking System, with the Payment Engine performing real-time validations and funds availability checks through integration services. Under Model II, the Payment Engine must include a Settlement Account Management module with an internal ledger that logs and maintains accurate, up-to-date debit and credit entries for all settlement accounts, ensuring proper accounting and reconciliation for all transactions. All account-related actions must be secured, logged and auditable. Bidders must describe the validation and funds-check flow, including applied rules, fallback handling in case of temporary core-banking or network unavailability.

Multiple Settlement Accounts per Participant

The Payment Engine must support the maintenance and operation of multiple settlement accounts per participant. The system shall allow configuration of separate accounts by currency, business line, purpose, or ancillary system. It must enable account-level limits, liquidity segregation, and reporting, ensuring that debit and credit operations, queuing and liquidity reservations can be executed and monitored independently for each account. The Payment Engine shall provide real-time balances across all participant accounts and allow authorized users to transfer liquidity between their own accounts intraday, subject to applicable authorization and control rules. Bidders shall describe the configuration approach, accounting treatment, and operational monitoring associated with multiple

account management, and the mechanisms that enable authorized liquidity transfers between accounts intraday under applicable authorization and control rules.

Scheduling for Insufficient Funds and Timed Payments

When a payment received by the Payment Engine cannot be settled due to insufficient funds, it must be placed in an intraday queue, where transactions are ordered according to their execution priorities and, for payments with equal priority, on a first in first out (FIFO) basis, taking into account the release time (if defined). The rules governing the placement and ordering of payments in the queue must be fully configurable. When payments are scheduled for a future date, or a specific release time, the system must manage their orderly execution using configurable scheduling logic. Bidders shall describe how transactions are scheduled, queued, prioritized, and retained, and explain whether the system supports dynamic prioritization (automatic adjustment of priorities based on liquidity or timing conditions), automatic reordering, and time-based reattempts. The solution must also provide mechanisms for authorized users (both participants and Central Bank operators) to manually change the position of a transaction in the queue or revoke (cancel) a queued transaction prior to settlement, in accordance with applicable business and authorization rules.

Automatic Reprocessing of Scheduled Transactions

Queued transactions must be automatically reprocessed when settlement conditions are met, including cases when sufficient funds become available or when offsetting or liquidity-optimization mechanisms enable execution. Bidders shall describe the logic governing reprocessing, including retry intervals, prioritization criteria, triggers from offsetting or gridlock resolution routines, and any applicable manual override capabilities.

Rejection and Scheduling for Insufficient Funds

If a participant's account has insufficient funds to complete a transaction, the system must queue the payment and periodically recheck the possibility to settle the queued transactions throughout the day or when funds become available. Transactions that remain unsettled by the End of Day must be automatically rejected unless explicitly warehoused for the next business day under defined business rules, with full audit logging of authorization and status. At Start-of-Day, unsettled warehoused transactions must be automatically reactivated for settlement, subject to the applicable business rules, timing constraints, and liquidity conditions. Warehousing of unsettled payments must be configurable based on multiple criteria, such as payment priority, payment type (e.g. MPI related, budget payments). Bidders shall describe the queuing and monitoring mechanisms, the frequency and conditions of queue rechecks, and the process by which unsettled payments are either rejected or warehoused, including how unsettled warehoused transactions are authorized, stored, and reactivated on the following business day.

Settlement Prioritization

The solution must support settlement prioritization based on configurable criteria, such as SWIFT priority codes or participant- or system-specific rules. Bidders shall explain how priority levels are defined, enforced, and integrated into the queuing and settlement processes, and clarify whether

prioritization is static (rule-based) or dynamic, where priorities may automatically adjust in response to liquidity conditions, timing constraints, or operator intervention.

Priority Classification of Payments

The solution must support classification of payments into the predefined priority categories specified by the Central Bank and apply these consistently across all workflows. Bidders shall describe how these priority categories are configured, how they influence settlement sequence, and the rules governing the processing of urgent or time-critical payments. Settlement prioritization must support at least three levels of priority: High-Value Payments (HVP), Urgent (URGP), and Standard (SSTD), as described in Chapter 4 Core Banking and Payment Engine Interaction Models Description. Bidders shall indicate whether prioritization logic can be configured independently by the Central Bank and how it is applied dynamically within the queuing and settlement processes.

Liquidity Reservation and Configurable Usage Rules

The Payment Engine must allow the reservation and allocation of liquidity for high-priority or time-critical payments, such as for High Value Payments (HVP) and Urgent (URGP) categories. Liquidity reservation for defined priority could be set on 'standing order' mode or 'current reservation' mode, and reservations must be capable of being modified or deleted. The system shall enable the Central Bank to configure rules governing the amount, duration, and conditions of reserved liquidity, ensuring that priority transactions can be executed under liquidity constraints. Liquidity usage parameters, including thresholds, and release conditions, must be fully configurable and adjustable in real time by authorized users. The Payment Engine shall provide continuous visibility of available, reserved, and utilized liquidity by participant, account, and currency, and ensure that all liquidity movements are logged, auditable, and reflected immediately in settlement and reporting views.

Value Dating and Cut-Off Handling

The system must provide functionality to manage cut-off times and value dates consistently across currencies, payment types, and participants. Cut-off handling defines the latest time by which a payment instruction can be accepted for same-day settlement, while value dating ensures that payments are settled on or after their effective settlement date. Bidders shall explain how the solution enforces cut-off times, processes or rejects transactions submitted after cut-off, and automatically adjusts or validates value dates when required (for example, moving to the next business day in case of holidays or after cut-off submission).

Value Date Verification

The Payment Engine must validate value dates associated with each payment order, ensuring that expired or future-dated transactions are rejected or warehoused as appropriate. Bidders must explain how value dates are checked, the rules applied for acceptance or rejection, and how the system processes transactions with valid future dates once they become eligible for settlement, including the treatment of warehoused payments across business days.

Scheduled Payment Order Acceptance Rules

The Payment Engine must apply explicit business rules to determine whether scheduled payment orders (future-date or time-specified transactions) are acceptable for future settlement. At the time of submission, the system must validate that such instructions meet all applicable criteria, including permitted value date range, payment type eligibility, participant authorization, and successful completion of technical and business validations. Bidders must explain the rules governing acceptance and warehousing of scheduled orders, the treatment of non-compliant instructions (e.g. immediate rejection or operator review), and the process by which such payments may be resubmitted or automatically reprocessed at the next business day.

End-of-Day Cut-Off Management

The Payment Engine must enforce configurable cut-off times for payment submissions and settlement cycles, defining the transition from regular settlement to end-of-day processing. Bidders must describe how cut-offs are applied, how late submissions are handled, with the CBA having flexibility to configure different cut-offs for various payment types, currencies or participants. The Payment Engine must also support defined exceptions for settlements permitted after standard cut-off. Bidders shall explain how such exceptions are configured, authorized, and monitored within the system.

Offsetting of Scheduled Payments

The Payment Engine must support automatic bilateral and multilateral offsetting of queued transactions. The system must include a configurable bilateral offsetting mechanism, ensuring that both payments are executed only if neither account becomes negative after settlement. When the counter payment is at the top of the queue, balance control may be bypassed according to defined rules. The solution must also support multilateral netting during the day to prevent gridlock and at End-of-Day to optimize liquidity settlement. Gridlock prevention procedures must be capable of being activated automatically based on configurable conditions or manually by authorized Central Bank users within risk management procedures. The offsetting mechanism must allow configuration of execution priority, queue handling (e.g. FIFO or bypass), and applicability for single or multiple payments. Bidders shall describe the logic used to detect and settle offsetting payments, how this process interacts with prioritization and scheduling mechanisms, and the extent to which the offsetting principles, parameters, and triggers are configurable by the Central Bank.

Multi-Currency Capability

The Payment Engine must support multi-currency processing. Bidders shall describe how the Payment Engine handles currency-specific rules, account structures, and real-time settlement processes across different currencies, and disclose any functional or technical constraints related to multi-currency operations.

Ancillary Systems Settlement

The Payment Engine must support continuous (24/7/365) clearing and settlement with designated ancillary systems, including ArCa and STAK. This includes the processing of defined ISO 20022-AM net

settlement messages, execution of daily clearing cycles, management of liquidity reservations, and integration with each ancillary system's settlement mechanism. Bidders shall describe how their solution implements and supports ancillary system settlements, what types of settlement procedures are supported, how settlement reconciliation workflows are configured and monitored, and which types of ancillary systems their solution currently supports, such as card-based or other retail payment system, as well as DvP or PvP settlements.

Outbound Message Creation after Settlement

Upon completion of each settlement, the Payment Engine must automatically generate and transmit outbound messages confirming transaction status, accounting entries, liquidity updates, and if necessary, containing inbound message details. These messages shall be sent in real time to all relevant recipients, including Core Banking System. Outbound messages shall be produced in ISO 20022-AM or non-ISO 20022 XML format, following predefined templates. The system must ensure reliable delivery, audit logging, and traceability of all outbound messages, including retries and confirmation acknowledgements where required.

Group Payments and Configurable Rules

The Payment Engine must support the processing of group or bulk payment messages, allowing individual payment instructions to be submitted, validated and settled within a single grouped transaction. The system shall apply configurable business rules governing acceptance, sequencing, prioritization, and liquidity usage for such grouped payments. Bidders shall describe how grouped payments are configured, managed, and monitored, including exception handling at both group and transaction level.

5.1.2 Risk, Compliance & Oversight

Risk Management

The Payment Engine must provide real-time monitoring and control of credit, liquidity, and operational exposures, supporting continuous oversight by the Central Bank. The system must prevent transactions that would exceed approved participant limits, including intraday credit, overdraft, and liquidity thresholds, and must automatically trigger alerts and blocking actions when such thresholds are reached. It must provide real-time reporting and audit visibility of participant positions, exposures, and risk events. Governance and authorization controls must ensure that any limit adjustments, overrides, or exception handling are fully logged and subject to Central Bank approval. The solution must allow the Central Bank to define, adjust, and configure all relevant risk parameters, including limits, reservations, thresholds, and alerts.

Early Warning & Alerting Framework

The Payment Engine must include an early warning and alerting framework that provides automated, real-time notifications to Central Bank operators and system participants. Bidders must describe how

the solution detects and issues alerts for risk limit breaches, liquidity shortfalls, operational incidents, or abnormal transaction patterns. In the case of liquidity shortfalls, the framework must also detect and report the resulting accumulation of transactions in the payment scheduler that are waiting for available funds. Bidders should also explain how alerts are logged, audited, and integrated into the broader risk management and oversight functions.

Overdraft and Intraday Credit Facility Management

It is preferable for the CBA that the provided Payment Engine solution supports the available balance management functionality, as well as the definition and management of configurable overdraft limits and intraday credit facilities. Such facilities must be governed by rules defined by the Central Bank, including eligibility criteria, credit limit levels, collateralization conditions (if applicable), and repayment or limit reset procedures at the end of day. The Central Bank must be able to configure, adjust, and monitor these parameters.

Overdraft Extension Notifications

For the solution supporting overdraft and credit facilities the Payment Engine must notify both market participants and the Central Bank in real-time when overdraft limits or intraday credit facilities are extended, reduced or otherwise adjusted. Notifications must include the updated limit values, be available through both user interfaces and system-to-system channels (e.g. APIs or message-based integration) and be logged with audit trails. Bidders must describe how such notifications are triggered, delivered, and recorded, and how they integrate with the overall credit and liquidity risk management framework.

PFMI Compliance

The solution must be fully aligned with the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs) as published by the Bank for International Settlements (BIS). Bidders must detail how the system design, operational processes, and controls support compliance with PFMI standards, including settlement finality, participant default management, liquidity and credit risk frameworks, operational resilience, and data confidentiality.

Security & Compliance

The Payment Engine must comply with recognized information security standards (e.g. ISO/IEC 27001) and incorporate multi-factor authentication (MFA), role-based access control (RBAC), and auditable security controls. Bidders must describe how compliance is achieved and maintained, including certification status, governance, and audit mechanisms.

Regulatory Oversight Tools

The Payment Engine must provide integrated tools to facilitate regulatory oversight, stress testing, and supervisory reporting. Bidders must describe built-in functionalities for simulating stress scenarios

(e.g. participant default, liquidity shortages, system outages) and for assessing systemic impact. The solution must generate automated reports aligned with Central Bank and international regulatory templates and support dashboarding, as well as provide APIs for data extraction.

Market Infrastructure Monitoring

The Payment Engine must monitor connected market infrastructures, such as securities settlement and card clearing systems, covering settlement flows, message exchanges, and reconciliation status. The system must generate real-time alerts for delays, failures, or mismatches, and make such alerts and notifications available only to authorized users through both user interfaces and system-to-system channels. Bidders must describe the scope and granularity of monitoring, including how integration with external infrastructures and Central Bank oversight systems is achieved, and how monitoring data is secured and audited, and how this data can be presented for operational and regulatory purposes.

Cross-Border Transfer Compliance

For transfers involving Loro/Vostro accounts or other correspondent arrangements, the Payment Engine must capture and display both originating and destination countries of the transaction to support AML/CFT monitoring, sanctions screening, and regulatory reporting. Bidders must describe how this data is captured, validated, and made available for compliance analysis and supervisory oversight.

KYC Assessment

The Payment Engine should support integration of KYC data for participant onboarding and, where relevant, transaction screening. The system must enable validation and maintenance of KYC information, support integration with external compliance systems, and ensure secure storage with full audit trails. Bidders must describe how KYC data is managed and applied in payment processing and oversight.

5.1.3 Participant Model & Sponsorship

Participants Management

The Payment Engine must provide comprehensive participant management capabilities, including the definition and maintenance of participant types, eligibility criteria, onboarding and offboarding procedures, configurable access levels and permissions, transaction and operational limits, compliance monitoring, and full audit and reporting functionality for all participant-related actions.

Indirect Participants

The Payment Engine must support indirect participants operating through direct participants, ensuring that all transactions initiated by indirect entities are processed, settled, and reported under the account and responsibility of their sponsor. The system shall maintain a configurable sponsor to participant

relationship framework defining eligibility, limits, and access rights. It must ensure that transaction routing, liquidity usage, and settlement reporting accurately reflect these relationships. All indirect participant activities must be fully traceable and accessible to authorized users, including participants, sponsors, Central Bank operators, and comply with settlement, audit, and reporting requirements.

5.1.4 Operational Features

Alerts & Notifications

The Payment Engine must generate real-time alerts and notifications based on configurable thresholds, acceptable risk limit breaches, or system events, and ensure their secure delivery to authorized parties and users. Bidders should explain delivery channels, escalation paths, and integration with external monitoring systems.

Reporting & Analytics

The Payment Engine must generate both real-time and scheduled reports, accessible through dashboards and be exportable in common formats. Reporting must cover operational, liquidity, and participant activity aspects, including but not limited to intraday liquidity positions, queue and settlement statistics, and system performance metrics. Where applicable, the system should also support Cash Pooling or liquidity concentration reports, summarizing participant balances across multiple accounts. The Payment Engine must allow authorized users to create new customized report forms, define report parameters, and design layouts without requiring vendor development. Bidders must describe available standard reports, options for ad hoc and custom report creation, supported output formats (e.g. CSV, PDF), frequency options, and distribution channels (e.g. UI, API, secure file transfer).

Usage Metrics

The Payment Engine must track and report system usage across participants, user groups, transaction types, and defined time periods. Bidders must explain how usage metrics are collected, visualized, and made available for operational oversight and billing purposes.

Monitoring & Dashboards

The solution must provide real-time monitoring dashboards for central bank operators, offering visibility into system health, transaction processing, and SLA adherence. Bidders must describe available monitoring metrics, alert configurations, and dashboard customization.

Main Account Monitoring

The Payment Engine must provide secure, real-time monitoring of all accounts relevant for payment processing, including main accounts and settlement accounts in accordance with both models (see Chapter 4 Core Banking and Payment Engine Interaction Models Description). Authorized users must

be able to view the account inflows, outflows, and balances across these accounts, including detailed listings of debit and credit transactions with timestamps and amounts. Each participant must likewise have the ability to monitor its own account balances, transaction activity, and payment queue status in real time through secure access channels. Accounts unrelated to payment processing should not be visible unless explicitly authorized. Bidders shall describe how these monitoring capabilities are delivered, the level of data granularity available, and the mechanisms ensuring accuracy, timeliness, and access control.

Operational Analytics

The Payment Engine must provide real-time and historical analytics of operational KPIs (e.g. throughput, retries, queue times, settlement delays, SLA adherence). Dashboards must support trend analysis, drill-down investigation, and correlation with system events to support proactive operations and incident resolution. The analytics framework must allow data export or integration with standard Business Intelligence (BI) and IT Monitoring tools (e.g. data visualization and performance monitoring platforms) through standardized interfaces. Bidders must describe available analytics features, customization options, and supported integration mechanisms.

Payment Repair and Recall

The Payment Engine must support controlled mechanisms for correcting, cancelling, or recalling payment instructions. Cancellation or revocation refers to payment instructions that have not yet been settled, allowing authorized users to cancel queued or unsettled payments in accordance with Central Bank policies. Recall refers to a transaction that has already been settled, where the system must enable initiation of a recall request and allow the recipient to either accept and execute a return payment or reject the recall request. The system may allow authorized repair of incomplete or invalid payment instructions prior to settlement without full resubmission, provided that all actions are fully logged and auditable. Bidders shall describe the repair, cancellation, and recall workflows, authorization requirements, audit trail controls, and how these functions ensure compliance with settlement finality principles.

Intraday Liquidity Alerts

The Payment Engine must generate intraday liquidity alerts (e.g. low balances, threshold breaches) and ensure their secure delivery to authorized users and parties. Alerts must be available through both user interfaces and system-to-system channels. Bidders must describe supported alert types, configurable thresholds, delivery methods, and access control mechanisms.

Real-Time Payment Tracker

The solution must enable end-to-end tracking of payments, including timestamps, status updates, and reason codes, accessible to both Central Bank operators and participants according to their authorization levels. Bidders must describe how the tracker integrates with settlement processes, participant interfaces, and regulatory reporting.

Application & Infrastructure Monitoring

The Payment Engine must provide built-in monitoring of its application components, supporting infrastructure, and directly connected interfaces, covering availability, performance, error conditions, and capacity utilization. The system must provide real-time alerts, maintain detailed event logs, and be able to integrate with Central Bank's enterprise monitoring tools for centralized oversight. Bidders must describe the scope of monitored parameters, alerting configuration, and escalation mechanisms or integration possibilities.

Cash Forecasting

The Payment Engine must provide cash forecasting tools to enable market participants and the Central Bank to project intraday liquidity positions based on historical payment flows, scheduled transactions, expected settlement activity as they can be used to predict current flows, flag low transactions volumes/values, and highlight potential issues with market participant sending capabilities. Bidders must describe available forecasting models, visualization options, and how forecasting integrates with liquidity monitoring and reporting.

Transaction Cancellation and Dispute Management

The Payment Engine solution must provide functionality to cancel transactions that have been sent but not yet settled, subject to applicable authorization rules and time constraints. In addition, the system must include built-in communication channels that allow participants and the Central Bank to initiate, track, and resolve transfer disputes or refund requests. Bidders should describe the cancellation workflow, including approval requirements, settlement cut-off considerations, and audit trails, as well as the tools available for managing dispute resolution and refund processes.

Instant Payments and Ancillary System Readiness

The Payment Engine architecture must support future integration with instant payment services and additional ancillary systems through standardized APIs and modular components. The design must enable seamless interoperability with both domestic and cross-border payment infrastructures and support extension of settlement and monitoring functions to 24/7/365 environments. Bidders shall describe the solution's current readiness and roadmap for instant payments adoption, including integration with Core Banking System, change-management approach, and adaptability to new ancillary systems introduced in the future.

Billing & Invoicing

The Payment Engine should include usage-based billing and invoicing capabilities, with customizable rate structures, reporting, and integration with external accounting systems. Bidders must describe billing logic, invoicing frequency, and reconciliation features, as well as describe how the Payment Engine billing function can support billing for transactions and services provided outside of the Payment Engine.

Fee Management

The Payment Engine should provide configurable fee management, allowing the Central Bank to define participant-specific pricing rules, exemptions, and discounts. The system must support flexible fee calculation based on transaction type, value, volume, or participant category. Bidders must describe how fee rules are configured, updated, applied in real-time, and reported to participants.

Fee Invoicing & Reconciliation

The Payment Engine should generate periodic invoices, statements, and fee reports, and deliver them through UI and system-to-system channels. The Payment Engine must support reconciliation of market participant payments against billed fees with full audit trail. Bidders must describe invoice formats, delivery methods, and reconciliation features.

Fee Dispute Management

The Payment Engine should provide workflows for managing billing and fee disputes, allowing market participants to submit claims, Central Bank staff to approve or reject adjustments, and all actions to be logged with audit trails. Bidders must describe how disputes are logged, processed, and resolved.

Multilingual Support & Unicode Compliance

The solution must provide multilingual user interface and must include mandatory support for the Armenian language. Standardized coding systems and Unicode compliance must be supported to enable accurate rendering of multiple languages and character sets. Additionally, the solution must support multiple languages for notifications, alerts, and message content, allowing users to select their preferred language. Bidders must describe available language packs, font management capabilities, and any limitations in multilingual deployment or support.

End-to-End Message Lifecycle Traceability

The Payment Engine must offer full lifecycle traceability for each message, from receipt or creation to successful delivery to the designated recipient (e.g. Core Banking, Messaging Service). Traceability must cover message receipt, validation, queuing, processing, acknowledgment, transmission, and final delivery events, with precise timestamps for each stage. The system must support UETR (Unique End to End Transaction Reference) for messages received via SWIFT and generate UETRs for messages sent through SWIFT channels to ensure global traceability and reconciliation. The Payment Engine must allow retrieval and reprocessing of messages that failed or were delayed, enabling operators to review complete transaction histories and re-initiate processing or controlled re-sending after resolving the root cause (e.g. connectivity loss of configuration error). Access to traceability functions must be role-based. Each participant must be able to trace only their own messages, while the Central Bank operator must have the ability to trace and manage all messages across the Payment Engine. Bidders must describe available tracking and user interface capabilities, including options for search, filtering, audit logging, reprocessing, and controlled message re-sending.

Timestamped Processing Logs and Retention
The Payment Engine must maintain detailed, timestamped logs for all message processing activities, including execution of scheduled tasks (such as Start-of-Day, End-of-Day, or cut-off processes) and real-time transaction processing steps. Logs must be securely stored and protected against unauthorized access or modification. The system must support configurable retention policies aligned with regulatory and operational requirements and include automated archival procedures. Logging must cover both operational events such as routing, validation, queuing, acknowledgments, failures, and recovery activities, and user or participant actions, such as manual resubmissions, annotations, configuration changes, and administrative operations. The level of logging details must be configurable to balance operational visibility, system performance, and storage efficiency. Bidders must describe how logging accuracy, security, and retention are managed, including configuration options and compliance controls.

Administrative and System Event Logging
The solution must log administrative actions and message filtering configurations. Logging must also capture configuration changes, API calls, retries, and system failures, with secure access controls. In addition, the solution must record user-related activities such as user creation and modification, role and permission delegation, changes to access rights, and user operations performed within the system. Bidders must describe audit scope, accessibility, and reporting features for administrators.

Participant-Facing Help Desk Services

The Payment Engine could provide (or be able to integrate with) a Help Desk module that allows market participants to submit and track requests, report incidents, and receive status updates in real-time. The module must support automated ticketing, escalation workflows, notifications, and audit trails. Bidders must describe how the Help Desk operates, how market participants interact with it, and how it integrates with Incident Management.

Message Storage & Traceability
The Payment Engine must maintain a centralized repository for storing all processed messages and related operational events, with full search, filtering, viewing, and export capabilities. Operators must be able to access both sent and received messages and export search results, with all export actions securely logged and governed by role-based permissions managed by the Information Security (InfoSec) function. Filtering must support parameters such as message type, participant, status, unique number, date/time, with the ability to export filtered results. The repository must also retain event logs, allowing users to view and filter by event type, user, and time, and export results as needed. Archive management features must allow messages and related data to be moved from the main archive to a deleted archive and restored if required. The solution must comply with configurable data retention and audit policies, including long-term and legal archiving as defined by CBA requirements (e.g. minimum of 5 years).

Data Accessibility and Integration Across Components
The Payment Engine must support secure, structured data storage and provide standardized access mechanisms (e.g. database views) to enable centralized data retrieval. Bidders are required to ensure that the solution's components can expose data in a standardized, secure, and consistent manner to enable future integration. Data must be accessible without duplication and must support reporting, monitoring, and regulatory compliance. Long-term retention and efficient retrieval must be adaptable to the Central Bank's operational and regulatory context.

Message Format Interoperability and Participant Format Identification
In the transition period the Payment Engine must determine compliance with the applicable format based on the participant (whether the participant has already migrated to ISO 20022 standard or still uses legacy format). Bidders must describe how coexistence between legacy and ISO 20022 messages is managed to ensure consistent validation, traceability, and interoperability.

Internal Message Format Interoperability
The Payment Engine must support message exchange with internal systems (e.g. Core Banking and other CBA systems) using both ISO 20022-AM and non-ISO 20022-based XML formats according to predefined templates. The Payment Engine determines the required message type and initiates the appropriate message.

5.1.5 Reference Data

Reference Data Management (RDM)
The Payment Engine must provide user interaction capabilities for the creation, amendment, validation, and authorization of standing and reference data (e.g. participants, users, accounts, static data tables). The solution must enforce role-based access controls, support maker-checker approval workflows, and provide full audit trails. It must integrate with the designated master source, ensuring automatic synchronization, validation, and consistency of shared data across all integrated components. The system must support both import and export of reference data allowing seamless updates between the Payment Engine and external systems. Bidders must describe how reference data is maintained, updated, and propagated across the system in real time, and data integrity is ensured.

Standing Orders and Act-on-Behalf Configuration
The Payment Engine must support the definition and maintenance of standing orders (such as scheduled liquidity transfers or other periodic settlement-related operations), as well as act-on-behalf rights. These functions are particularly relevant under Model II but may also apply to other operational models. Please refer to Chapter 4 Core Banking and Payment Engine Interaction Models Description. Authorized users must be able to create, modify, and approve such instructions within a controlled configuration environment. All standing orders and act-on-behalf arrangements must be validated, securely stored, and be fully auditable. The system must manage these configurations within the Reference Data Management (RDM) framework through the user interface.

5.1.6 Scheduling

Scheduler Functionality

The Payment Engine must provide a scheduling functionality to manage time- and event-based operations, such as value-dated payments, cut-off enforcement, and periodic or recurring system tasks. The scheduler must support configurable event timing, sequencing and exception handling, including the execution of Start-of-Day, End-of-Day, and intraday processes. The solution must support Start-of-Day and End-of-Day processing with configurable timings and procedures supporting both Models as described in Chapter 4 Core Banking and Payment Engine Interaction Models Description. It must also provide business day and calendar management capabilities, including defining business days, operating times, and public holidays, handling sudden changes, and notifying users of calendar updates. Bidders must describe the scheduler's configuration flexibility, monitoring and control tools, how it ensures reliable and timely execution of all critical operational activities.

Differentiated Cut-Off Times by Message Type and Associated Systems

The Payment Engine must allow configuration of distinct cut-off times for different message types (e.g. interbank and customer payments), as well as for associated ancillary systems such as ArCa and the Central Depository. The system must also ensure differentiated cut-offs by currency and participant, ensuring that settlement cycles align with the operational requirements for various market infrastructures and participant groups.

Payment Scheduling through the User Interface

The Payment Engine user interface must allow authorized users to schedule future-dated or time-triggered payment instructions, including liquidity transfers or standing settlement orders. The UI must support the definition of execution dates, release times, and recurrence rules, with appropriate validation and approval controls. Bidders should describe how scheduling is configured and authorized through the user interface, how it integrates with system-level scheduling mechanisms, and what safeguards ensure accurate timing, authorization, and auditability of scheduled transactions.

5.1.7 Data Warehouse & Querying

Data Warehouse (DWH) User Interaction

The Payment Engine must provide user access to data warehouse functions, enabling query, reporting, and historical data analysis. The system must support predefined regulatory and operational reports, ad hoc queries, and export to standard formats. Bidders should describe how the data warehouse is accessed, secured, and refreshed, including query performance and scalability.

Query Capabilities

The Payment Engine must provide real-time query and search functions across key data domains, including transactions, account balances, reference data, and system time. Queries must be available through both user interfaces and system-to-system channels, support multiple filtering criteria and return results with minimal latency. In Model II, queries on account balances must reflect settlement

account positions maintained within the Payment Engine, while in Model I they must reference main account balances retrieved from the Core Banking System. This approach is consistent with Main Account Monitoring, where balance visibility is model-dependent. The solution must ensure consistent and synchronized system time across all modules and interfaces. Bidders must explain supported query types, filtering and export options, synchronization mechanisms, and compliance with data security and access policies.

Search & Inquiry

The system must support real-time search and inquiry capabilities focused on transactional data including payment history, message details, and processing status. These functions must support operational monitoring and investigation, allowing authorized users to trace individual transactions and related messages. Access must be available both through the user interface and system-to-system channels. Bidders must describe query performance, supported filters, and security controls ensuring authorized and traceable data access.

5.1.8 Authorization & Approval Workflows

Approval Workflows

The solution must support configurable, multi-level approval workflows for payment processing and reference data maintenance. Approval rules must be role-based, enforce segregation of duties, and include secure electronic authorization mechanisms (e.g. digital signatures, certificate-based signing, or strong authentication) supported by comprehensive audit logs. The system must allow the Central Bank to configure the number of approval levels (e.g. maker-checker or multi-step approval), escalation paths, and monitoring capabilities according to operational policies. Bidders shall describe how approval workflows are defined, triggered and enforced across both payment and reference data processes.

User Roles and Access Model

The solution must provide a role-based access model to ensure secure and appropriate use of all system functions. Bidders should describe the role model in detail, covering functional roles and permissions, segregation of duties, and options for user management (e.g. creation, modification). The model must support both users within the Central Bank and market participants. Bidders must explain how the proposed solution supports role definition, administration, monitoring, and compliance with security and governance requirements.

5.1.9 User Interface Features

Web-based GUI and API Exposure

The solution must provide a dedicated, secure web-based graphical user interface (GUI), to enable operational monitoring and administration for the Central Bank and market participants, applicable to the Payment Engine. The GUI must offer real-time visibility into message traffic, transaction queue,

account balances, liquidity positions, limits, and reservations, as well as processing statuses. It must enable users to perform authorized operational tasks such as message replay, resubmission, prioritization, and queue management, and to exchange free-text correspondence, attach annotations, and upload supporting files. All functions available through the Web GUI must also be exposed via secure, documented API endpoints to enable integration with both the CBA Web Portal (in later phases) and participant applications. The GUI must be developed on a standardized, secure, and extensible architecture with role-based access control, callback mechanisms, and provisions for future enhancements. Bidders must describe GUI capabilities, API coverage and documentation standards, access control, and mechanisms ensuring security, extensibility, and interoperability.

Usability and Navigation
The Web GUI must provide an intuitive, user-friendly interface with configurable views, advanced filtering, and export options (e.g. CSV, PDF). It must support multi-lingual display and Unicode compliance to ensure accessibility for diverse users. Bidders should describe usability features, accessibility standards followed, and support for multi-language deployment.

Standing Orders, Recurring Instructions, and Liquidity Operations
The solution must enable authorized users to create, amend, and cancel standing orders, recurring and liquidity transfer instructions directly through the GUI, in line with the reference data definitions defined in Chapter 5.1.5. The interface must also allow authorized management of queued transactions, gridlock resolution actions, and prioritization of payments when liquidity constraints occur. Bidders must describe the configuration workflow for defining schedules, authorization and approval rules, and monitoring tools used to track the execution and status of standing or scheduled instructions.

Act-on-Behalf Functionality
The solution must allow the Central Bank, subject to proper authorization and reference data rights, to act on behalf of a participant to initiate, cancel, or where permitted, amend certain payment types before final settlement. Bidders must explain how act-on-behalf rights are configured, controlled, and audited, and how the functionality is made available through the GUI.

Participant and Reference Data Management
The Web GUI must enable authorized users to directly manage and edit reference data (e.g. accounts, participants, settlement instructions) with appropriate approval workflows and full audit trails. Bidders should describe how reference data is validated, authorized, and updated through the GUI.

Message and Account Monitoring
The Web GUI must allow both participants and Central Bank users to monitor transaction statuses and payment message processing stages in real time, including submission, validation, queuing, and settlement events. Account balance information must also be visible. If the Payment Engine performs accounting (Model II), balances must be displayed directly from within the Payment Engine; under

Model I balances must be retrieved from the Core Banking system. Please refer to Chapter 4 Core Banking and Payment Engine Interaction Models Description. The interface must support annotations and free-text correspondence on individual messages, as well as real-time event notifications (callbacks) through both the GUI and API to keep external systems updated on status changes. Bidders must describe monitoring granularity, event logging, and integration with alerting systems, and explain how balance data is sourced and displayed under different accounting models.

Customer Access Channels

The Payment Engine must support multiple secure access channels for participants, including a browser-based user interface, APIs, message exchange via Central Bank Gateway System, and secure file upload and download. The system must ensure consistent functionality, message handling, and data integrity across all channels, and provide fallback and recovery options in case a channel becomes unavailable. Bidders shall describe the supported access and authentication methods including multi-factor authentication (MFA) capabilities, and the measures implemented to ensure channel resiliency and continuity.

5.2 Integration Functional Requirements

5.2.1 General Integration Requirements

Messaging Format and Interfaces

The Payment Engine shall support ISO 20022 and non-ISO 20022-based XML message formats according to predefined templates for inbound and outbound messages. Bidders shall present a complete ISO 20022 message list detailing inbound and outbound message types and describe how the solution processes and creates non-ISO 20022-based XML messages. Message flows, transformations, and acknowledgements must be fully auditable, ensuring end-to-end integrity, traceability, and compliance with non-ISO 20022-based XML and ISO 20022 standards.

Real-Time Integration via APIs and Message Queues

Bidders must demonstrate how the solution supports real-time integration using APIs, message queues, and either industry standard mechanisms such as file-based interfaces or event-driven architectures. The solution must handle both synchronous and asynchronous messaging patterns and ensure low-latency performance under production-scale workloads, consistent with the transaction volumes and operational demand of a national Payment Engine environment. Real-time queue interfaces must provide message history, content viewing, and message counters to enable operational monitoring and troubleshooting across inbound and outbound message flows.

Connector Availability for Existing Systems

Bidders must provide details on available out-of-the-box or toolkit-based connectors for integration with existing CBA systems (e.g. Core Banking, GSASS, Gateway). All connectors should be customizable and designed for secure, upgrade-safe deployment with minimal operational disruption.

Bidders must clearly describe the recommended integration approach including supported protocols, message formats, and data exchange mechanisms.

Integration with Internal Compliance and Screening Systems
The solution must support bidirectional integration with existing and future internal compliance systems, such as AML and sanctions screening, to ensure compliance checks as part of transaction processing. The Payment Engine shall enable message exchange with these systems, while the compliance and screening logic remains in the respective internal systems. Bidders must describe integration methods, supported message types, and how mismatches or alerts are reported and remediated.

Reconciliation System Integration
The solution must support bidirectional integration with reconciliation engines to ensure accurate transaction matching between internal and external systems. The Payment Engine shall enable message exchange for reconciliation processes, including reporting of mismatches, exceptions, and remediation flows. Bidders must describe how reconciliation messages are generated, exchanged, and audited, and how integration ensures consistency across systems.

Regulatory Reporting Enablement and Schema Management
Bidders must describe how the solution supports routing, transformation, and delivery of regulatory reports compliant with standards such as ADF, XBRL, and ISO 20022. Mappings must be configurable given the possibility of expanding to support interoperability with other clearing and settlement schemas, and the solution must support updates to regulatory schemas with minimal disruption or manual intervention.

5.2.2 RTGS-Specific Integration Requirements

Ancillary System processing support
The Payment Engine must support the specific processes related to the ancillary systems e.g. STAK, ArCa, and related payment subsystems through standardized, well-documented interfaces. The system must allow the definition and maintenance of ancillary participant data, settlement parameters, and processing rules within the reference data module. Bidders should describe how ancillary system interactions are configured, monitored, reconciled, and controlled for consistency and auditability.

Payment Engine-Core Banking integration

Bidders must indicate whether the solution supports both interaction models (please refer to Chapter 4 Core Banking and Payment Engine Interaction Models Description) and describe technical and business flows, transaction execution and liquidity management processes for both models. Bidders must also describe settlement, posting, reconciliation and exception handling procedures under each model. All postings must be validated against accounting rules, logged with full audit trails, and alerts must be generated for mismatches or posting failures

In addition to these models, the Bidder may provide variations to both interaction models with clear identification of benefits of such variants. In case the Bidder provides a modified interaction model, they should clearly explain how the suggested model addresses all requirements described in this ToR.

Offline Balance

The solution must offer the possibility to support offline balances in the situation where the Core Banking system is not available, e.g. during an incident or End-of-Day processing. The Bidder must describe the process of copying balances from the Core Banking system and updating the balances while processing the transactions. At the end of the off-line period the system must perform transaction loading and reconciling the balances back to the Core Banking system.

6 Non-Functional Requirements

6.1 Performance & Reliability

High Throughput
The solution must support high volumes of messages (60k payments processing per hour), including large-format and nested structures, with proven benchmark results (i.e. maximum number of messages processed per hour). Performance must remain consistent regardless of message size or complexity. Bidders must provide benchmark details and describe optimization techniques and any limitations when handling complex message types.

Low Latency
The solution must ensure consistent low transaction processing latency across all stages of the settlement workflow, including validation, queuing and posting, even during peak load conditions. Bidders must provide benchmark data (average and peak latencies in seconds/minutes), describe key factors influencing latency (e.g. message size, encryption, or transaction volumes), and outline available optimization mechanisms.

Scalability & Performance Management
The solution must be designed to scale seamlessly in response to growth in transaction volumes, participant numbers, and message traffic, without degradation of performance, stability, or latency. It must support both vertical and horizontal scaling across components, enabling flexible resource allocation and capacity expansion as needed. Bidders must describe how scalability is achieved, coordinated, and monitored across all components to maintain end to end performance and resilience, and provide indicative benchmarks or client references demonstrating proven scalability in production environments.

Monitoring & Bottleneck Detection
The solution must allow both business monitoring (e.g. detection of unusual payment behaviour) and technical monitoring (system performance issues such as CPU, memory, I/O, network and throughput). It must provide real-time tracking with configurable thresholds, automated alerts, dashboards, and diagnostics, as well as integration and remediation capabilities. Monitoring must provide an integrated view across components, allowing unified tracking of message flows, latency, and failure points.

Graceful Degradation
The solution must support resilience patterns and failure isolation such as circuit breakers, bulkheads, and retry logic to maintain critical operations when under strain. Bidders must describe configuration options, fallback behaviour, and any limitations in degraded modes.

Maximum File Size Handling
The solution must support the upload, processing, and validation of large individual files up to 99MB without performance degradation or data loss. Bidders must provide benchmark results demonstrating consistent throughput and stability when handling files at or near this maximum threshold.

6.2 Resilience & Availability

SLAs & Uptime
Bidders' solution must commit to a minimum of 98% uptime (average over a 3-month period), supported by formal SLAs that cover monitoring, redundancy, incident response, and documented escalation procedures. Bidders must also outline service credits or penalties for SLA breaches.

High Availability
The solution must ensure uninterrupted operations through active clustering and seamless failover, including during planned maintenance activities, without service interruption. The solution must support a Recovery Time Objective (RTO) of less than 1 hour and a Recovery Point Objective (RPO) of less than 5 minutes. Bidders must detail backup, replication, and synchronization mechanisms to guarantee these objectives.

Disaster Recovery
The solution must include a geographically separate disaster recovery site with real-time or near-real-time data synchronization, automated failover, and clearly defined RTO/RPO to ensure business continuity without data loss. Bidders must describe synchronization methods, failover and failback procedures, testing frequency and methodology, and how the solution ensures uninterrupted transition between primary and disaster recovery sites during both planned and unplanned events.

DR Testing
Bidders must provide evidence from recent DR test reports of the proposed solution, including scope, scenarios, RTO/RPO results, and outcomes, with reference to compliance standards (e.g. ISO 22301). Evidence should also note frequency, validation, and corrective actions.

Coordinated Release and Upgrade Cycles
The solution must support synchronized upgrades and configuration changes across components to ensure operational continuity and consistency of business processes. Upgrades or configuration changes must not result in partial downtime, inconsistent message states, or data loss. The solution should enable phased or rolling updates, allowing critical functions to remain online during maintenance activities.

Stress Resilience
The solution must demonstrate stability under extreme load conditions, with stress test results showing throughput, latency, resource utilization, and system behaviour under saturation. Bidders must describe testing scope, tools, frequency, and any performance limits identified.

Automated Failover & Message Rerouting
The solution must support real-time failover with automated message rerouting to alternate nodes or data centres, ensuring zero data loss and no disruption to transaction processing. Bidders must describe failover detection, switchover procedures, deployment models, and any limitations.

7 Technology & Architecture Requirements

Bidders shall submit detailed solution architecture documentation, including high-level and component-level architecture diagrams as part of their proposal. Such documentation is required to understand how the proposed solution will align with Central Bank's Financial Market Infrastructure goals.

7.1 Hardware Layer

Server Infrastructure
The solution must support deployment on enterprise-grade rack-mounted, blade, and hyper-convergent servers. Bidders must specify compatibility, performance benchmarks, and recommended configurations for production-scale workloads.

Network Infrastructure
The solution must integrate seamlessly with industry-standard routers, switches, and firewalls. Bidders must describe supported network topologies, high-availability options, and redundancy mechanisms.

Storage Systems
The solution must support SAN and NAS storage architectures with high-performance, fault-tolerant access. Bidders must provide details on supported storage protocols, scalability, and data protection mechanisms.

Backup and Recovery
The solution must integrate with enterprise backup solutions (e.g. HPE backup systems) to ensure secure, reliable data backup and restoration. Archive functions must support recovery of deleted or archived messages, including restoration from a deleted archive back to main archive. Bidders must describe supported backup strategies, archiving (when the data moves from back-ups to the archive) & retention policies, and recovery time objectives (RTO) for back-ups and retrieving/accessing archived data.

Operating System & Hardware Compatibility
The solution must support deployment on industry-standard enterprise operating systems, including Microsoft Windows Server. Bidders must specify the minimum and recommended hardware requirements (CPU, memory, storage, and network specifications) for production-scale deployments. The response must also confirm whether the solution is certified or tested for operation on Microsoft OS environments.

7.2 Infrastructure Layer

Virtualization Compatibility
The solution must support enterprise virtualization platforms including VMware ESXi, Hyper-V, Nutanix. Bidders must describe resource optimization, VM management, and high-availability features.

Containerization and Orchestration
The solution must support Docker containers with orchestration by Kubernetes (K8s). Bidders must demonstrate automated deployment, scaling, self-healing, and lifecycle management capabilities.

Operating System Support
The platform must support deployment on Microsoft Windows Server and enterprise Linux distributions Bidders must specify supported OS versions, kernel requirements, and certification status.

7.3 Platform Layer

Relational Database Support
The solution must support enterprise-grade relational databased management systems (RDBMS), preferably Microsoft SQL Server and/or Oracle, which are the platforms currently used by the Central Bank. Bidders must describe supported high-availability configurations, backup and recovery mechanisms, and database migration strategies. If an alternative RDBMS is proposed, Bidders must demonstrate equivalent functionality, security, and performance, and provide a clear migration or interoperability approach.

Database Access for OLAP & OLTP
The solution must provide secure access to the underlying database to support both OLTP (Online Transaction Processing) and OLAP (Online Analytical Processing) capabilities. This must enable real-time monitoring, transaction statistics gathering, and analytical reporting without impacting core transactional performance. Bidders must describe supported access methods, security controls, performance isolation mechanisms, and how analytical workloads are managed alongside transactional operations.

DevOps & CI/CD Integration
The solution must integrate with CI/CD pipelines and infrastructure-as-code (IaC) tools. Bidders must describe build automation, version control, and deployment workflows.

Monitoring & Observability
Bidders must provide details on built-in monitoring, logging tools (Zabbix, Microsoft SCOM), and alerting capabilities, including system health checks, transaction metrics, and error rate reporting. Integration with Prometheus, Grafana, or equivalent third-party tools must be supported. The solution must enable users to build custom dashboards and configure alerts for proactive monitoring and diagnostics.

Business Intelligence and Analytics
The solution must integrate with SAP BusinessObjects Business Intelligence Suite. Bidders must specify supported analytics use cases, report generation, and data source integration. (Data Warehousing to be provided by CBA.)

Integration and Middleware
The platform must support enterprise-grade integration with existing and future middleware and enterprise service bus (ESB) solutions used by the Central Bank. It must be compatible with common ESB architectures and standard integration patterns. Bidders must describe supported integration patterns, messaging protocols, fault tolerance.

Collaboration & Messaging Platforms
The solution must interoperate with the Central Bank's existing collaboration and messaging platforms, including (if applicable) systems such as HCL Domino, HCL Notes, or Microsoft Exchange. Bidders must describe supported messaging APIs, authentication methods, and security controls.

7.4 Application Layer

Backend Technology Support
The solution should preferably support development and deployment of applications using widely adopted backend frameworks such as .NET Core or provide equivalent capabilities that enable seamless integration with CBA's existing and future technology landscape. Bidders must describe API management and supported standards for SOAP and RESTful APIs, including details of any alternative frameworks if .NET is not supported.

Frontend Technology Support
The solution must support modern web UI frameworks. It must also integrate with UI libraries such as Bootstrap. Bidders must describe cross-browser compatibility, responsive design, and accessibility compliance.

Deployment Flexibility
The solution must support deployment across on-premises, private cloud, and hybrid environments with seamless migration or configuration options. Bidders should specify supported models and limitations.

Extensibility
The solution must support extensibility through API gateways, plugin frameworks, and event hooks to enable custom integrations and workflows without modifying core code.

Extensibility & Customization
The solution must provide SDKs, APIs, and plugin frameworks for business logic customization, including low-code/no-code support and safe version management.

Simulation Environment
The solution must provide a non-production environment that mirrors production to validate new message types, formats, and workflows safely. Bidders must describe simulation capabilities, synchronization with production, available tools, and any functional limitations.

8 Security Requirements

8.1 Operational Security

Access Control and Permissions
The solution must provide granular, role-based access control (RBAC) with dynamic permission management by user type, system role, or operational domain. All access events and permission changes must be logged with user identity, timestamp, and action details to ensure full traceability. The solution should support integration with enterprise identity and authentication mechanisms (e.g. Active Directory, SAML, OIDC) and enable multi-factor (MFA) authentication for privileged administrative accounts.

Custom Role and Duty Segregation
The solution must support the creation and management of custom roles in addition to predefined ones and allow modification to predefined roles where necessary. It must enable flexible permission configuration to align with organizational structures, operational policies, and regulatory requirements.

Network and Transport Encryption
The solution must support encryption of all communications and data exchanges, including APIs and administrative interfaces, using TLS 1.3 or higher (or an equivalent secure protocol). Private keys must be protected with hardware-based cryptographic modules (HSMs or tokens) and never stored in plaintext. Bidders must describe key management processes, including key generation, rotation, distribution, and revocation.

Message-Level Electronic Signature
The Payment Engine must support message-level electronic signing and verification for both inbound and outbound payment messages, ensuring non-repudiation and message integrity from Central Bank Gateway System to Payment Engine and vice versa. The solution must support CBA approved hardware and software-based electronic signature management tools, including integration with the local HSM for signature generation and verification. Bidders must describe how message signing and verification are implemented, managed, and audited end to end.

Encryption at Rest
The solution must implement encryption at rest for all sensitive data repositories, including databases, backups, and audit logs using strong algorithms such as AES-256 or equivalent. Bidders must describe key lifecycle management processes, including secure generation, rotation, and destruction. Integration with centralized or hardware-based key management systems is desirable.

Certifications & Data Sovereignty
Bidders must list all relevant cybersecurity and privacy certifications currently held (e.g. ISO/IEC 27001, SOC 2 Type II or FIPS 140-3) and confirm compliance with applicable local data protection and cybersecurity laws, including data residency or sovereignty obligations. Additional certifications or attestations (e.g. ISO/IEC 27701, PCI DSS, GDPR alignment) are desirable.

Solution Capability (Risk Visibility and Control Management)
The solution must provide capabilities that support the organization's cyber-risk governance, including audit-ready reporting and dashboards for security events, configuration posture, and compliance status. It must support integration with enterprise GRC or risk register tools through APIs or data export, enable user activity logging and analytics for control verification, and allow alignment of policy enforcement and configuration baselines with the organization's ISMS. The solution should also provide configurable alerting thresholds and periodic compliance summaries to support management review.

Cyber Incident Response
The solution must provide technical capabilities to support incident detection, analysis, containment, and recovery, including, centralized logging and event correlation interfaces, secure APIs for integration with SIEM, SOAR, and ticketing systems, role-based access controls to isolate compromised accounts or services, and support for evidence preservation through log export and forensic data collection. The solution must offer configuration options to automate response actions such as blocking, quarantine, or service restart through standardized integrations. Support for automated threat indicators (STIX/TAXII), playbook execution, or SOAR interoperability is desirable.

Cyber Resilience and Recovery
The solution must be architected for resilience against cyberattacks, including ransomware, denial-of-service, and data corruption scenarios. It must support secure backup, replication, and restoration of critical data and configurations, ensuring integrity, authenticity, and minimal recovery time (RTO/RPO). Backups and recovery artifacts must be encrypted and protected against unauthorized modification or deletion. The solution should include mechanisms for rapid isolation or failover, such as redundant nodes, immutable storage, or snapshot rollback.

Privilege Access Management
The solution must provide built-in mechanisms to control and audit privileged access to administrative interfaces, including system consoles, management APIs, configuration panels, and service accounts. It must support role-based administrative segregation between security, operations, and audit functions, and enforce least-privilege principles through granular access controls, time-limited or workflow-approved privilege elevation, and strong multi-factor authentication (MFA) for all administrative actions. Comprehensive, immutable audit logs of privileged activity must be maintained and exportable to the organization's SIEM for correlation. Integration with enterprise PAM solutions (e.g. CyberArk, BeyondTrust, Thycotic, HashiCorp Vault) must be supported via standardized protocols such as RADIUS, LDAP, or REST API.

Security Monitoring and Logging
The solution must provide continuous security monitoring to detect anomalies, unauthorized access, and indicators of compromise. All security-relevant events must be logged in an immutable, tamper-resistant format and integrate with the enterprise SIEM via standard interfaces (e.g. Syslog, JSON, or API). Bidders must configure and maintain monitoring, alerting thresholds, and event correlation rules, ensuring timely review and escalation of alerts. Support or behavioural analytics, AI-based anomaly detection, or SOAR integration is desirable.

8.2 Cybersecurity & Resilience

Governance Framework

Bidders must demonstrate alignment with established cybersecurity and risk management frameworks such as NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, or equivalent standards. Bidders must maintain enterprise-level information security governance, including a documented and approved security policy, clearly defined roles and escalation paths, and a risk management methodology aligned with ISO 31000/ISO 27005 principles. Evidence of assurance activities (e.g. internal audits, certification audits, SOC 2 reports) must be provided. Continuous improvement mechanisms (e.g. KPIs, KRIs, or OKRs) are desirable to demonstrate active maturity management.

Security Monitoring and Threat Detection

The solution should maintain active monitoring of its managed infrastructure and services, including detection and triage of potential security incidents affecting the solution. Bidders should operate or integrate with a 24/7 Security Operations Centre (SOC) capable of monitoring, analysis and response. Bidders must describe the monitoring scope, alert escalation process, and communication workflow with CBA in case of anomalies or confirmed incidents. Use of threat intelligence feeds and periodic tuning or detection rules is desirable.

Cyber Incident Response

Bidders must maintain a formally documented and approved Cyber Incident Response Plan (IRP) outlining procedures for detection, escalation, containment, eradication, recovery, and post-incident review. The IRP must clearly define responsibilities, communication channels, and escalation paths, including coordination with CBA's incident management process. Bidders must provide evidence of regular vulnerability scanning, penetration testing, regular incident response exercises, and tracking of corrective actions. Reporting obligations to CBA must be met within SLAs or regulatory timeframes. Integration with CBA's IRP and incident communication workflows should be supported.

Cyber Resilience and Recovery

Bidders must maintain and periodically test documented cyber-resilience, disaster recovery, and business continuity plans to ensure uninterrupted operations during and after security incidents. These plans must address critical services, communication procedures, and clearly defined recovery time objectives (RTOs) and recovery point objectives (RPOs) aligned with CBA's resilience expectations. Bidders must provide evidence of regular recovery testing, including backup restoration validation, ransomware-simulation drills, and corrective action tracking. Coordination with CBA's continuity and crisis management framework must be demonstrated through defined notification and escalation procedures. Independent assessments or certifications (e.g. ISO 22301) are desirable.

Third-Party and Software Supply Chain Security

Bidders must maintain a formal Third-Party Risk Management and Supply Chain Security Program aligned with recognized ISO/IEC or NIST. This program must include processes for supplier risk assessment and due diligence prior to onboarding, contractual cybersecurity requirements ensuring confidentiality, integrity, and availability of CBA data, ongoing supplier monitoring and annual re-assessment, third-party incident reporting obligations with defined breach-notification timelines, and subcontractor flow-down clauses to ensure equivalent security standards. Bidders must provide evidence of vendor-risk assessments for key suppliers supporting this solution. Certification under ISO/IEC 27036 or NIST SP 800-161 is desirable.

Secure Software Development and Supply Chain Integrity

The solution must be developed and maintained in accordance with secure software development lifecycle (SSDLC) practices, incorporating security by design, code review, and dependency control. It must provide verifiable assurance of software integrity through digitally signed source code and binaries, verified update packages (e.g. code-signing, checksum validation), and a Software Bill of Materials (SBOM) detailing all third-party and open-source components, their versions, and licensing. The solution must support automated vulnerability scanning and dependency monitoring throughput the build and deployment pipeline, as well as secure update mechanisms resistant to tampering and downgrade attacks.

Vulnerability and Patch Management

Bidders must maintain a documented vulnerability and patch management process covering all components of the proposed solution, including operating systems, middleware, databases, and third-party libraries. The process must define clear timelines for applying patches by severity (e.g. critical within 72 hours of release) and include continuous vulnerability scanning with periodic remediation reports to CBA. Emergency patching procedures, rollback testing, and change-control approvals must be clearly defined. The solution must support secure patch deployment mechanisms such as code signing, validation, and rollback. Integration with vulnerability management platforms (e.g. Tenable, Qualys, OpenVAS) is desirable.

Privileged Access Management

Bidders must operate and maintain a corporate privileged access management (PAM) program covering all systems and infrastructures used to deliver, host, or support the proposed solution. All privileged accounts under the Bidder's control must be managed through a secure PAM platform with credential vaulting and automatic rotation, session recording and monitoring, and dual-approval or break-glass procedures for emergency access. Bidders must provide evidence of PAM policy enforcement, including periodic access reviews and revocation of dormant or shared credentials. All privileged sessions involving CBA data or environments must be fully auditable and attributable to individual identities.

Data Loss Prevention

Bidders must implement and operate controls to prevent unauthorized disclosure or exfiltration of CBA data from any environment where it is hosted or processed. These controls must include DLP

monitoring of data in motion, at rest, and in use; content inspection with contextual policy enforcement; encryption or tokenization of sensitive fields; and restrictions on removable media and external file transfers. Bidders must classify and label sensitive data in alignment with CBA's data-classification policy. Integration with enterprise DLP or CASB tools for centralized visibility and control is desirable.

Secure API Management

The solution must enforce strong API-level security controls, including authentication, authorization, rate limiting, input validation, and encryption of all API traffic. APIs must be protected against injection, replay, privilege escalation, and denial-of-service attacks in line with OWASP API Security Top 10 recommendations. Bidders must maintain documented API security practices covering key management, version control, change approval, and vulnerability testing. APIs must provide standardized audit logs for integration with SIEM/SOC systems. Support for mutual TLS, OAuth 2.0/OpenID Connect, and signed tokens (JWS/JWT) is desirable.

Business Continuity and Crisis Communication

Bidders must maintain and regularly test Business Continuity and Crisis Communication Plans (BCP/CCP) aligned with ISO 22301 and the CBA's continuity framework. These plans must define recovery time objectives (RTOs), recovery point objectives (RPOs), and fallback procedures to ensure service availability during cyber incidents or infrastructure failures. Bidders must conduct at least one full-scale test per year, complemented by periodic partial or scenario-based tests, and provide documented evidence of test results and corrective actions. Clear communication protocols with the CBA must be established for incident notification, escalation, and stakeholder coordination, including regulators and critical participants. Integration of BCP with the Bidder's incident response and disaster-recovery processes is required.

9 Qualification and Other Relevant Requirements

9.1 General Eligibility Criteria

This RFP is open to solution providers with demonstrated expertise in:

- Deploying Central bank–grade RTGS solutions;
- Implementing ISO 20022-compliant messaging and settlement workflows;
- Designing secure, scalable, and high-availability payment infrastructure; and
- Integrating RTGS solutions with payment gateways, and global financial networks.

9.2 Bidder's Qualification Criteria

RTGS Deployments
The solution provider must demonstrate proven experience in at least three RTGS system implementations for central banks. Bidders shall provide detailed information on each deployment, including the project scope, implementation timeline, and the type of financial market infrastructure served. For each reference, Bidders must indicate what Core Banking (General ledger) -RTGS interaction model (as described in Chapter 4 Core Banking and Payment Engine Interaction Models Description) was implemented, provide brief description for each solution, and summarize key lessons learned. It's preferrable to describe implementation cases with different interaction models.

Central Bank References and Case Studies
Bidders must supply contactable references and detailed case studies from central bank deployments, including comprehensive project summaries, implementation challenges overcome, measurable outcomes achieved, and direct contact details for verification. References must be authorized and available for direct *contact during the evaluation period*.

Bidder Recognition and Listings
The Bidder must be listed in CBA vendor rosters, approved technology lists, or recognized in major industry reports and publications (e.g. IMF, BIS, World Bank). Bidders must provide specific recognitions, industry certifications, published case studies, participation in standard-setting bodies, or citations in research publications that validate their market position and expertise.

Long-Term Client Relationships
Bidders must demonstrate strong client retention over 5+ years with major financial institutions, showing evidence of successful contract renewals, service expansions, technology upgrades, and continuous partnership value. Bidders must provide examples of long-term engagements including client testimonials, retention rates, and evidence of successful platform evolution within existing relationships.

Project Failures or Security Incidents
Bidders must disclose any publicly known project failures, legal disputes, or security incidents

including data breaches or operational disruptions, along with resolution outcomes and lessons learned. Preference is given to those with no unresolved incidents or ongoing contractual disputes.

9.3 Account Management and Project Team Qualification Requirements

Account Management, Governance, and Executive Engagement
Bidders must maintain a skilled account management team with structured governance models and executive-level client engagement. Clear organizational structure, team qualifications, and governance frameworks implemented for similar clients must be described in detail.

The bidder must demonstrate the capability to provide a qualified, experienced, and well-structured team to ensure effective project delivery, governance, and executive-level client engagement.

Qualified Project Personnel
The bidder must allocate qualified and experienced personnel capable of fulfilling all contractual obligations and ensuring that project objectives (timeline and quality) are achieved.
Team members involved in the implementation must have demonstrated experience executing similar large-scale projects with relevant technical, managerial, and domain expertise required for the project.
As evidence of compliance, the bidder must submit CVs of all key experts, including supporting documentation confirming qualifications and certifications;

Language and Communication Requirements
All team members must have at least working proficiency in English.
Knowledge of Russian is desirable.

9.4 Financial Standing

Financial stability
Bidders must present evidence of their financial stability over the last 3 years and forecast for 2026, demonstrating consistent financial performance, liquidity, and capital adequacy to sustain long-term contractual obligations. The required evidence shall include, at a minimum:

- International network audited financial statements for the last three fiscal years (2022, 2023, and 2024). Audited financial statements must be issued by an independent audit firm applying internationally recognized auditing standards. If requested audited financial statements are not available, unaudited financial statements must be provided;
- Interim financial statements or management accounts for 2025;
- Banking references or letters from financial institutions confirming the Bidder's financial soundness, resilience, and ability to meet long-term contractual commitments.

All documents submitted must be clear, complete, and issued or signed by authorized entities (auditors, financial institutions, or rating agencies). The CBA reserves the right to request additional clarification or supporting documentation as needed.

9.5 Cost & Licensing

Upfront Licensing Costs
Bidders must specify the upfront licensing costs associated with the proposed Payment Engine. Bidders should also provide details of any relevant pricing tiers, thresholds applicable to the licensing structure.

Implementation Cost Breakdown
Bidders are required to submit a detailed breakdown of the total implementation cost. This should include all activities necessary to operationalize the Payment Engine, such as software configuration, system integration, customization, project management, testing, and support during the deployment phase. In addition to listing all required licenses (e.g. Operating Systems, MS Queries), Bidders must also provide the corresponding licensing costs for these components. Each component should be described with sufficient clarity to demonstrate how the cost relates to the project scope.

Ongoing Support and Maintenance Costs
Bidders must outline the annual costs associated with support and maintenance of the deployed solution over a minimum period of 10 years. This should include standard support charges, upgrade entitlements, security patching, bug fixes, version enhancements, SLA commitments, and delineation between what is covered under standard versus premium support tiers. Bidders must also clearly delineate the scope and pricing of standard vs premium support tiers, ensuring that long-term maintenance and upgrade obligations are fully covered within the proposed support model.

Infrastructure Requirements and Associated Costs
Bidders must provide a clear summary of the hardware, storage, network, and operating system requirements to deploy the solution. The proposal must distinguish between primary and disaster recovery environments and state whether Bidders offer cloud or on-premises deployment options. If cloud deployment is proposed, it should primarily be positioned for testing, non-critical, or lower-tier environments. Associated costs for each infrastructure model should be outlined clearly, including third-party software licenses if applicable.

Modular Licensing Structure
Bidders must specify whether the licensing allows modular acquisition of features, such as separate licensing for reporting modules. The proposal must state whether these modules can be licensed independently or only as part of a bundled suite.

Licensing for Non-Production Environments
Bidders should indicate their standard approach to licensing for non-production environments (test, development, training, disaster recovery).

Cost Breakdown and Transparency
An itemized cost sheet must be provided that includes all software license fees, professional services, testing environments, infrastructure requirements, documentation, and any additional costs expected to be incurred during implementation or support phases.

Visibility of Future Costs
Bidders must describe the mechanisms used to ensure predictability of future costs. This includes projected expenses for future upgrades, new features, user expansion, or institution onboarding etc. Bidders should explain how such changes are priced and how customers are informed of pricing impacts in advance.

9.6 Source Code Escrow Requirements

Source Code Escrow Agreement
Bidders must specify whether a source code escrow agreement will be provided for the proposed solution. The response should detail the frequency with which source code is deposited or updated, ensuring alignment with software release cycles.

Escrow Agent and Security
Bidders are required to identify the escrow agent used, including whether a third-party service is engaged. The proposal must provide information on the agent's reputation, reliability, and security measures in place to safeguard the deposited materials.

Escrow Agreement Structure
Bidders must confirm whether the escrow arrangement will be established as a tripartite agreement among the buyer, the bidder, and the escrow agent. The proposal should emphasize that such a structure is considered the most secure option.

Escrow Release Conditions
In case of Escrow Arrangement, bidders must define the conditions that would trigger release of the escrowed source code. These may include, but are not limited to, bidder insolvency, cessation of support, breach of contractual obligations, or failure to deliver agreed-upon services. The response should outline the process for invoking and executing such a release. Otherwise, the Bidder must specify alternative procedures that ensure the continued availability and operation of the solution

10 Implementation / Delivery

10.1 Proposed Implementation Roadmap

Bidders shall provide a clear, integrated, and practical roadmap for the implementation of the services included in this RFP:

- Real-Time Gross Settlement (RTGS) system.

The roadmap must cover the full project lifecycle from contract signing to final go-live. Specifically, the roadmap must include:

- A proposed implementation and delivery plan of key activities of the Payment Engine (e.g. change analysis, development, configuration, integration, installation, testing, commissioning, readiness acceptance, go-live, after care), and an indication of whether a parallel or sequential deployment is proposed;
- A proposed methodology and approach to identify gaps, configuration definitions and integration specifications including templates used, with explicit reference to how these align with the organization's SDLC (Software Development Life Cycle) and governance framework;
- A description of the development and configuration change management process and version controls, aligned with CMMI Capability Maturity Levels (CML) to demonstrate process maturity, governance, and continuous improvement;
- A rationale for the proposed sequence, including any benefits, the identification of delivery, technical, and operational risks with clear mitigation strategies, demonstrating proactive risk management, governance, and contingency planning;
- A proposed master test plan describing the tests performed by individual parties or combined, with alignment to SDLC quality gates and integration checkpoints;
- A proposed training plan, knowledge management and documentation plan must be provided to support the capture and transfer solution specific knowledge and documentation. Bidders must supply complete documentation, covering at a minimum: user manuals, detailed functional and technical specifications, operational and maintenance procedures, and training materials for different user groups (e.g. operators, administrators);
- A tentative timeline showing estimated durations and key milestones, with clear identification of:
    - Gap & Change Assessment
    - Delivery timelines for Development, Configuration/Customization, and Integration checkpoints
    - Environment readiness dates
    - Preparation of detailed test cases and execution of testing phases, including internal (CBA) and participant testing

  - Training phases
  - Final acceptance and operational readiness & transition
- A list of prerequisites, dependencies, and required inputs from the Central Bank of Armenia (CBA) and/or third-party vendors, including infrastructure provisioning, data readiness, technical resourcing, and institutional coordination.

The roadmap must support overall project planning, stakeholder alignment, and readiness tracking. It must be included in the Bidder's technical proposal and may be accompanied by a high-level Gantt chart or equivalent planning tool to illustrate proposed workstreams, timelines, and dependencies.

10.2 Implementation & Support

Training Approach and Coverage

Bidders must offer a comprehensive training plan including classroom, virtual, on-the-job, and e-learning methods. The training program should be adaptable to the Central Bank's operational and regulatory context with the specific scope, extent, and level of customization to be finalized during contract negotiation and the implementation phase.

Localized Training

Training materials must be localized and tailored to the central bank's specific implementation configuration, business processes, and regulatory environment. Materials must be available in local language where required and incorporate relevant local payment system examples, regulatory scenarios, and operational procedures specific to the Armenian market context.

Knowledge Transfer Strategy

Bidders must provide a detailed knowledge transfer plan enabling Central Bank teams to independently operate and maintain the system post-implementation. The plan should cover documentation with clear roles, timelines, and mechanisms to validate knowledge retention.

Support Availability

The solution must provide full 24/7/365 support, including during holidays and critical windows such as end-of-day processing, settlement cycles, and other high availability periods. Scheduled maintenance windows may be allowed but must be agreed in advance with the Central Bank and designed to minimize operational impact. Limited business-hours support will be considered inadequate for critical payment infrastructure.

Remote and Onsite Support Options

Bidders must describe support delivery models, including local presence capabilities, remote escalation paths, and scheduled onsite check-ins. The support model must include provisions for emergency onsite assistance within defined timeframes and local language support capabilities where required.

Release Frequency and Roadmap Sharing

Bidders must demonstrate a structured product development lifecycle with regular updates delivered

at least annually, including feature enhancements, performance improvements, and regulatory compliance updates.

Backward Compatibility of Releases

All new software releases must maintain full backward compatibility with existing configurations, interfaces, and data structures without requiring major system migrations or operational disruptions. Bidders must describe their compatibility testing processes, regression testing procedures, and rollback capabilities. Any breaking changes must be clearly identified with detailed migration paths and extended transition periods.

Realistic Delivery Timeline

Bidders must propose a realistic delivery timeline that accurately reflects project complexity, organizational readiness requirements, testing phases, and integration dependencies. Unrealistic commitments will be penalized. Timelines must include realistic allowances for user acceptance testing, parallel running, and staff training with appropriate contingency buffers.

Change Management and Version control

Bidders must provide a description of how the application development/evolution is managed in terms of delivering upgrades, how user requirements and market practice changes are incorporated into product evolution, and how version and quality control is implemented to ensure error free deployments.

11 Deliverables

11.1 Expected Deliverables and Planned Timelines

- The planned timelines are for guidance only. Participants must submit, in their proposals, a detailed schedule for contract execution, specifying all key phases and their respective target completion dates.

EXPECTED DELIVERABLES	PLANNED TIMELINES
• Delivery and Deployment of the System - All modules are installed, configured, and integrated.	• Up to XX months
•	•
• Training Course • - End-User Training for Supervisors, Analysts, and Administrators	•
• User Acceptance Testing (QA + UAT) - All functional and non-functional requirements have been validated.	• Up to XX months
•	•
• Pilot operation - Critical and key workflows are executed and demonstrated by real users.	• Up to XX months
• Final Delivery and Acceptance of the System	• Up to XX months
• Warranty period	•
• Technical Support and Maintenance	• In line with the timeline provided in the proposal

- The Bidder shall provide the Project roadmap and the Project Implementation Timeline.

If necessary, the Bidder must be physically present during the System deployment, acceptance testing, handover-acceptance, and training phases.

11.2 Project Documentation

Bidders shall create and maintain all project documents that shall be passed on to the Central Bank as deliverables as per the agreed project timelines. The documents created by Bidders will be reviewed and approved by the Central Bank.

The table below shows the minimum stages, activities and the associated deliverables for each stage:

Stage	Activities	Deliverables
Project Planning	• Project Planning and Management • Project Quality Assurance • Documentation of Project Plan	• Project Management Plan • Weekly and monthly status reports

Stage	Activities	Deliverables
	• Project Status Reporting	
Business and Functional Requirements Analysis	• International standards and practice assessment • In-depth analysis of business and functional requirement analysis • Stakeholders need analysis • Document final set of business requirements • Define and document functional requirements	• Benchmark review assessment report • Business Requirement Specification • Requirement Validation and Traceability Plan • Software Requirementsand Specifications Document
System Architecture Design	• Document a preliminary set of businessrules and workflows • Conceptual architectural system designmethodology • Develop a strategy to ensure a finalintegrated design • Documentation of a comprehensivedesign style guide • Prepare and develop strategy for design session results and validation of these results	• Solution Architecture • Information Architecture • Integration Architecture • Infrastructure Architecture • Security Architecture
Implementation	• Conduct ongoing reviews of the hardware and software performance andreliability to determine if hardware meets service level agreements. • Develop implementation strategy • Certify that the application, its domains, functions, data, processes, operationalprocedures, staffing and all other associated support are in operation • Chart contingency plans • Resolution of all issues • Approval of Project Team to move to the implementation phase of the project	• Application Implementation Plan • Release Notes
Testing	• Develop a strategy for testing the application processes and creating test environments and detailed test cases • Develop criteria for promotion	• Master Test Plan • System integration test cases • Test Protocol for Unit, Integration, and UAT stages • Performance MonitoringPlan

Stage	Activities	Deliverables
	from unit to integration test • Integration Testing • User Acceptance Testing (UAT) consisting of two phases: local testing by CBA, and participant testing • Demonstrate readiness for go-live after successful completion of UAT	• Performance, Volume and Stress Testing Reports
System Maintenance Support and Operations	• Stress Testing • Load Testing • Performance Testing • Make recommendations for changes to hardware or software requirements to improve performance • Documentation of the knowledge transfer materials that will be used toprovide orientation and kick-off for testing • Identification of the tools and reports thatwill be used to support all testing efforts • Steps to ensure any design changes arereflected in the test scripts system • Resolution of all issues identified as design issues • Resolution of all defects that prevent completion of test scripts • System Incident Resolution • Application Enhancements • Minor changes, bug fixes, errorresolutions and minor enhancements • Application Upgrades and updates • Apply regular patches	• System Integration Execution Report – on daily basis • System Maintenance and Support Plan • System Incident Resolution report • Adaptive Maintenance Report • Application • Enhancements Report
Training and Knowledge Transfer	• Documentation of the Knowledge Management Strategy • Documentation of the approach for evaluating the effectiveness of the knowledge transfer and training courses or sessions	• Knowledge Transfer and Training Plan • Training and Instructional Material • Application User Manual • Online User Aids

Stage	Activities	Deliverables
	• Documentation of the train-the-trainer strategy • Develop knowledge transfer programand classroom training materials • Conduct Trainings for all user groups (e.g. Central Bank operational staff, IT administrators, market participants) in accordance with the training plan approved by CBA, covering system functionality, operations, maintenance, and support procedures, as well as train the trainer sessions • Develop a methodology for reporting, reviewing, and improving knowledge transfer • Collect and monitor training feedback	

11.3 Acceptance Criteria

Acceptance will occur once the following conditions are met:

- All functional and non-functional requirements validated
- End-to-end integration tests passed
- DR failover demonstrated
- No Critical/High defects open
- Documentation approved
- UAT completion and sign-off
- Performance benchmarks achieved

12 Appendix

12.1 Acronyms

Acronyms	Full Names
ADF	Application Development Framework
AES	Advanced Encryption Standard
AM	Armenia e.g. ISO-AM
AMD	Armenian Dram
AML	Anti-Money Laundering
API	Application Programming Interface
AS	Ancillary System
BC	Business Continuity
BCP	Business Continuity Plan
BI	Business Intelligence
BIC	Bank Identifier Code
BIS	Bank for International Settlements
BM	BankMail
CASB	Cloud Access Security Broker
CBA	Central Bank of Armenia
CBDC	Central Bank Digital Currency
CCP	Crisis Communication Plan
CDA	Central Depository of Armenia
CFT	Combating the Financing of Terrorism
CI	Continuous Integration
CML	Capability Maturity Levels
CMMI	Capability Maturity Model Integration
CPMI-IOSCO	Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO)
CPU	Central Processing Unit

Acronyms	Full Names
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DR	Disaster Recovery
DvP	Delivery versus payment
DWH	Data Warehouse
EBRD	European Bank for Reconstruction and Development
EPS	Electronic Payment System
ESB	Enterprise Service Bus
FIPS 140-3	Federal Information Processing Standard 140-3
FMI	Financial Money Institution
GDPR	General Data Protection Regulation
GRC	Governance, Risk and Compliance
GSASS	Government Securities Accounting and Settlement System
GUI	Graphical User Interface
HPE	Hewlett Packard Enterprise
HSM	Hardware Security Module
HT	Armenian legacy message formats e.g. HT103, HT202
HVP	High Value Payments
IMF	International Monetary Fund
InfoSec	Information Security
I/O	Input/Output
IRP	Incident Response Plan
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO 20022	International standard for financial messaging
ISO20022-AM / ISO-AM	The ISO 20022-compliant usage guideline for Armenia (currently in the process of development)
ISO 22301	Business Continuity Management

Acronyms	Full Names
ISO 27001	International standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS)
ISO/IEC 27036	Supplier Relationship Security
ISO 31000/ISO 27005	International standard that provides principles and guidelines for effective risk management
ISO 9001	International standard that specifies requirements for establishing, implementing, maintaining, and continually improving a Quality Management System (QMS)
JSON	JavaScript Object Notation
JWS/JWT	JSON Web Signature / JSON Web Token
KPI	Key Performance Indicator
KRIs	Key Risk Indicators
KYC	Know Your Customer
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
MT/MX	Message Types (SWIFT messaging standards)
NBFI	Non-banking financial institutions
NIST	National Institute of Standards and Technology
OD	Operational Day
OIDC	OpenID Connect
OKRs	Objectives and Key Results
OLAP / OLTP	Online Analytical Processing / Online Transaction Processing
OS	Operating System
OWASP	Open Worldwide Application Security Project
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PFMI	Principles for Financial Market Infrastructures
PvP	Payment versus payment

Acronyms	Full Names
RA	Republic of Armenia
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-based access control
RDM	Reference Data Management
REST	Representational State Transfer
RFP	Request for Proposal
RTGS	Real-Time Gross Settlement
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAP	ERP system
SAML	Security Assertion Markup Language
SBOM	Software Bill of Materials
SDKs	Software Development Kit
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SIT	System Integration Testing
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation and Response
SOC 2	System and Organization Controls (Type 2)
SQL	Structured Query Language
SSDLC	Secure Software Development Lifecycle
SSS	Securities Settlement System
SSTD	Standard Payment
STIX	Structured Threat Information Expression
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAXII	Trusted Automated eXchange of Indicator Information

Acronyms	Full Names
TLS	Transport Layer Security
UAT	User Acceptance Testing
UETR	Unique End-to-End Transaction Reference
UI	User Interface
UN	United Nations
URGP	Urgent Payment
USD	US Dollar
VAT	Value Added Tax
XBRL	eXtensible Business Reporting Language
XML	Extensible Markup Language
XSD	XML Schema Definition

12.2 Definitions

Acronym	Full Names
CBANet	he CBA operates a global communication network CBANet - functions as a large Layer 3 (L3) infrastructure, fully administered and maintained by the CBA. CBANet is designed for financial institutions functioning within Armenia. Financial information traffic is transmitted between subscriber endpoint devices and the central node devices. Subscriber endpoint devices are installed at the premises of the respective institutions and are connected to their local area networks. The central nodes are located at CBA sites and aggregate information flows from all subscribers.
Technical Validation	Validation of the message structure, syntax, and format against the defined technical specifications and schemas (e.g. ISO 20022 XSD), including checks for message headers, envelopes, and mandatory fields
Business Validation	Validation of the message in the specific business context to ensure that all business rules and conditions are satisfied, for example verifying that the participant, account, payment type, and value date are valid and consistent with defined processing rules and limits
BankMail	The Financial Messaging System, which is currently in use

General Terms & Conditions (T&Cs)

DISCLAIMER:

(The Bidder acknowledges and agrees that this Public General Terms and Conditions ("General T&Cs") published by Central Bank of the Republic of Armenia ("CBA") in this Announcement shall form an integral part of any agreement, contract, or purchase order resulting from this tender process and shall not be subject of negotiation and/or revision by Bidder.

If the selected Bidder refuse to include these General T&Cs in the formal contract with CBA, or otherwise impede their inclusion, such refusal will be considered a rejection to enter into the contract in accordance with the Law of the Republic of Armenia on Procurement.)

1. Upon the award of the tender and execution of the formal implementation and deployment contract (hereinafter "Contract") between Central Bank of the Republic of Armenia (hereinafter "CBA") and selected Bidder (hereinafter also "Contractor"), the General T&Cs shall automatically be deemed incorporated into, and made binding upon, the parties as though fully set forth in the Contract.
2. The Contractor shall perform services strictly in accordance with General T&Cs, this Tender announcement, RFP and another relevant documents that are published, attached or referred by this Tender announcement ("Documentations").
3. The CBA accepts the following licensing model for the Real-Time Gross Settlement (RTGS) system (hereinafter – System):
   (a) Perpetual License or Similar License.

   The Contractor grants the CBA a perpetual, irrevocable, transferable (in the territory of the Republic of Armenia), and royalty-free license to use, install, and operate the software for the purposes prescribed by Documentations.
4. The Contractor represents and warrants that the software, license and the use thereof by the CBA, does not and will not infringe or misappropriate any copyright, patent, trade secret, trademark, or other intellectual property or proprietary right of any third party.
5. The Contractor shall indemnify, defend, and hold harmless the CBA, its affiliates, officers, employees, and agents from and against any and all losses, damages, liabilities, costs, and expenses (including reasonable attorney's fees) arising out of or relating to any claim, demand, or action by a third party alleging that the software infringes or misappropriates such third party's intellectual property rights. In the event of any such claim, the Contractor may, at its own expense and discretion:
   a) procure for the CBA the right to continue using the software;
   b) replace or modify the software so that it becomes non-infringing without materially affecting its functionality; or

c) if neither (a) nor (b) is commercially reasonable, terminate the license, service and refund to the CBA the prepaid fees for the remaining unused term.

6. The Contractor grants the CBA a right to configure, and integrate the provided software with the CBA's internal systems, databases, and third-party applications, for the purpose of enhancing functionality or interoperability, provided that such customization or integration:
    a) does not infringe upon any third-party intellectual property rights;
    b) is performed solely for the CBA's business purposes prescribed by Documentations; and
    c) does not result in the creation of a competing software or service.
7. The Contractor and the CBA shall attempt to settle any dispute resulting from the execution of the Contract amicably. Any disputes shall be subject to the exclusive jurisdiction of the London Court of International Arbitration. Any dispute, controversy, or claim arising out of or in connection with this Contract, including any question regarding its existence, validity, interpretation, performance, breach, or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause. The seat (legal place) of arbitration shall be London, England. The number of arbitrators shall be 1 (one) arbitrator. The language of the arbitration shall be English. The governing law of the Contract shall be the substantive law of laws of the Republic of Armenia.
8. The Contractor's and the CBA's liability is limited to the value of the Contract. Any other limitation of liability for parties shall not apply, until expressly agreed by the CBA.
9. In the event, when Contractor acts as vendor, distributor or agent of another company (producer company), which owns the license/software, the Contractor shall remain fully responsible to the CBA for all obligations set out in the Documentations and Contract. Nevertheless, nothing in these General T&Cs shall limit the CBA rights to claim against not only the Contractor but also the producer company, in its discretion.
10. CBA and/or Contractor can assign, mortgage, charge, or sub-license their rights only with written consent of the other party.
11. Nothing in the Contract shall prohibit the Contractor from granting licenses and the CBA from obtaining similar licenses/software with respect to the service and the software to other third parties.
12. If the Contractor provide Escrow agreement, at least the following trigger events shall apply:
    a) the Contractor is liquidated or otherwise dissolved; an order is made for the winding up of the Contractor, or the Contractor passes a resolution for winding up or is wound up whether compulsory or voluntarily (other than for the purposes of a solvent reconstruction or amalgamation); or the Contractor has a receiver appointed over all or any part of its assets or undertaking; or the Contractor becomes the subject of any business rescue proceedings or an

administration order, or enters into any composition or arrangement with its creditors; or any similar or analogous proceedings or event occurs in respect of the Contractor within the relevant jurisdiction;

b) The Contractor files a voluntary petition or otherwise seeks relief under any bankruptcy, insolvency, or similar law;

c) The Contractor has been declared bankrupt or has been granted suspension of payments, either by involuntary or voluntary proceedings.

13. Where the Contract refers to terms and conditions available on websites, the Contractor agrees that only the version of such terms attached to the Contract shall apply. Future changes on website shall not apply to the Contract unless expressly approved in writing by the CBA. In the event of any conflict, inconsistency, or ambiguity between such terms and conditions, and the Documentations, the Documentations shall prevail and govern.
14. The Contractor shall not use, display, reproduce, reference, or otherwise make use of the CBA's name, trademarks, service marks, trade names, logos, branding elements, or any other identifiers ("Marks") in any marketing materials, case studies, press releases, customer lists, presentations, proposals, websites, or any other public communications without the CBA's prior written consent, which may be granted or withheld at the CBA's sole discretion.
15. Contract shall have the following contractual clauses for the termination by the CBA: The CBA shall have the right to terminate the Contract, in whole or in part, by written notice to the Contractor, if the Contractor:

    a) materially breaches any provision of the Contract and fails to remedy such breach within 15 (fifteen) business days after receiving a written notice specifying the breach;
    b) fails to render/deliver any part of the System during the term of the Contract,
    c) suspends the performance of the Contract for any reason not connected to CBA's fault,
    d) fails to ensure that the software complies with the technical specifications, performance indicators, security requirements, or other criteria set out in the tender Documentations or the Contract, and does not remedy such non-compliance within the period specified in the Contract;
    e) fails to provide maintenance, updates, patches, or support services in accordance with Documentations and the Contract, causing disruption to the CBA's operations or preventing the intended use of the software and does not remedy such scenarios within the period specified in the Contract;
    f) delivers software containing repeated, critical, or unresolved defects that materially affect its use, performance, or availability, and does not correct such defects within the timeframe established by the Contract;
    g) violates confidentiality, data-protection, information-security, or access-control requirements of the CBA;

h) engages in conduct contrary to applicable law or fails to comply with mandatory regulatory requirements relevant to the performance of the Contract; or

i) through any action or omission, creates a material risk to the CBA's business continuity, system stability, data integrity, or the security of the CBA's IT infrastructure.

In such cases, termination shall become effective upon the date specified in the CBA's written notice, and the Contractor shall be obligated to promptly refund to CBA all payments received at the date of such termination. All such refundable amounts shall be reimbursed to CBA within 15 (fifteen) business days of receipt of written notice from the CBA. The Contractor refund obligation shall apply regardless of any costs incurred by the Contractor and shall be without prejudice to any other rights or remedies available to CBA under this Contract or by law.

T&Cs of Payments and delivery models

16. The total price of the System (including license, software, maintenance, support) provided by Contractor is final and the Contractor cannot impose additional costs. for updates, patches, fixes, or required third-party components. The Contractor reconfirms that the CBA shall not pay any additional fee for any feature of the software.
17. The Contractor who submits positive audited financial statements that meet the Purchaser's requirements (see ToR Section 9.4) shall be eligible for the following 2 (two) phased payments.

a) Advance Payment

Up to 25% of the total implementation cost (Contract price) may be paid as an advance payment according to Part 8 and the Appendix 3.1 of the invitation.

b) Go-Live Payment

The Go-Live payment shall be deemed payable only upon the Contractor's full and satisfactory completion of all work prescribed in the Contract and the CBA's written Act of Acceptance of the System, following all required testing, review, validation procedures, acceptance criteria set out in the Documentations. The Act of Acceptance should be duly signed by the parties. The payments to Contractor shall be made within 10 (ten) working days after mutual sign off of the relevant Act of Acceptance.

18. The Contractor acknowledges that any payment by the CBA cannot be made earlier than December 2026 (in accordance with the requirements of Article 15 part 6 of the Law of the Republic of Armenia "On Procurement"). The Go-Live date cannot be earlier than January 2027.

19. The Contractor that does not demonstrate financial standing as described above (didn't submit positive audited financial statements) shall be eligible only for the total Contract price after the written Act of Acceptance of the System. In other words, no advance or milestone payments will be provided, and whole payment shall be made solely upon Go-Live.
20. Contractor shall be responsible for providing the simulation mechanisms and acceptance tools required to organize and perform acceptance testing independently of the other systems.
21. The deliverable package and acceptance criteria for each implementation stage shall be defined and negotiated on the basis of the work breakdown structure proposed by the Contractor in its RFP response and shall become an integral part of the Implementation Roadmap. The following items constitute a mandatory, but not exhaustive, list of deliverables to be included in each package:
    a) the deliverable itself;
    b) a delivery description and complete package inventory;
    c) test reports, including internal functional, non-functional, and regression (where applicable) testing;
    d) simulation mechanisms and acceptance tools required to organize and perform acceptance testing independently of the other system components;
    e) load test reports (where applicable);
    f) vulnerability assessment and penetration testing protocols (where applicable);
    g) deployment and configuration instructions;
    h) integration points configurations instructions - documentation and functional connections to existing systems and external parties (where applicable);
    i) migration instructions (where applicable);
    j) internal and external user guides (where applicable);
    k) IT support manuals and operational guides;
    l) training materials and training sessions (where applicable);
    m) signed support and maintenance contract (applicable only for the Go-Live).
22. The acceptance process shall be formalized and binding for both Parties. The acceptance procedure shall include:
    a) the CBA shall have a formally defined and limited period *(to be agreed and specified in the Contract)* to review and accept each deliverable package;
    b) The CBA shall document all identified comments, defects, and issues as part of the acceptance process'
    c) The Contractor shall have a defined and limited timeframe (to be agreed and specified in the Contract) to fix all blocking and critical issues identified during acceptance.
23. If blocking or critical issues are not corrected within agreed and specified timeframe, the respective stage shall be considered not accepted.

T&Cs of Implementation Roadmap.

24. The project roadmap proposed in the RFP response by Contractor, as subsequently refined during the negotiation phase and aligned with the final scope of work, actual start and final dates, shall form an integral part of the Contract as the Implementation Roadmap.
25. The Contractor shall be fully responsible and liable for complying with all timelines, milestones, and deadlines set forth in the approved Implementation Roadmap. Implementation RoadMap shall be subject to strict monitoring and control. The Contractor shall immediately notify the CBA in writing of any circumstances that may affect its ability to meet the agreed deadlines. Such notification shall not release the Contractor from its obligations under the Contract unless expressly agreed to in writing by the CBA.
26. The Implementation Roadmap shall be consistent with the tentative timeline proposed in the Contractor's RFP submission. Any deviation from the proposed timeline shall not exceed 30% of the originally proposed durations. The final completion date shall not be later than December 31, 2027.

T&Cs of Penalty Calculations.

27. Any failure by the Contractor to meet the deadlines or milestone dates specified in the Implementation Roadmap—unless caused by Force Majeure or by the CBA's written instruction or CBA's fault—shall constitute a contractual delay. In such cases, the Contractor shall be subject to delay penalties. In case of violation of the Implementation Roadmap (included interim and final deadlines) by Contractor, CBA reserves the right to claim a penalty in the amount of 0.1 (one tenth) per cent of the amount payable at the given stage/phase prescribed by Implementation Roadmap for each overdue day.
28. In case of violation of the payment terms specified in the Contract and upon written request of the Contractor, Contractor reserves the right to claim a penalty in the amount of 0.1 (one tenth) per cent of the amount payable at the given stage/phase prescribed by Implementation Roadmap for each overdue day.
29. The CBA's decision not to immediately impose penalties shall not be construed as a waiver of its right to enforce the penalty provisions at any later time.
30. The imposition of delay penalties shall be without prejudice to any other rights or remedies available to the CBA under the Contract.
31. The CBA has a right to make direct deductions of penalties from the payments payable to Contractor.

T&Cs of Project management Governance

32. Operational-Level Meetings. The Contractor shall organize regular operational-level meetings, held no less frequently than once every two weeks, to update the CBA on the current status of work, plan upcoming activities in detail, and highlight any emerging

issues or risks. The CBA may request additional operational-level meetings when reasonably necessary, including in response to urgent issues, changes in scope, or material risks.

33. Steering-Level Meetings. The Contractor shall organize regular steering-level meetings, held no less frequently than once every month, to inform the Project Sponsor and Product Owner on project progress and to address any issues or risks that cannot be resolved at the operational level.
34. The Contractor shall ensure the attendance of personnel with appropriate technical and managerial authority to address operational matters, resolve issues, and make necessary decisions. The Contractor shall prepare and circulate relevant materials, including progress reports, updated schedules, risk assessments, and any other documentation reasonably required by the CBA prior to each meeting.
35. The Contractor shall not transfer, assign, or otherwise delegate its responsibilities, obligations, or deliverables under the Contract to any third party, whether in whole or in part.
36. In all circumstances, the Contractor shall remain fully accountable to the CBA for the satisfactory and timely performance of all deliverables under the Contract, irrespective of any assistance obtained from third parties.

T&Cs of Support and Maintenance

37. The Contractor shall provide 12 (twelve) month warranty for the System starting from Go-Live date ("Warranty Period").
38. During this Warranty Period, the Contractor shall, at no additional cost to the CBA, perform all necessary repair and corrective actions required to restore the System to the level of functionality existing on its respective Go-Live date.
39. Contract should include a clause, that parties agree to sign a separate support and maintenance contract. Support and maintenance contract shall include the availability of all essential functions of the System, updates, security patches, technical support, documentation, and interoperability measures necessary to maintain the System in good working order.
40. The support and maintenance contract will be signed for a minimum of 10 (ten) years starting from Go-Live.
41. The support and maintenance contract shall include
    a) fixed pricing for the first 3 (three) years, with procedures for price revision for each next 3 (three) year's period with up to 20% adjustment limit (compared to the previous period price),
    b) minimum support service levels and maintenance conditions

    consistent with those proposed in the Contractor(s)' RFP submission.
42. The Contractor and the CBA shall attempt to settle any dispute resulting from the execution of the support and maintenance contract amicably. Any disputes shall be

subject to the exclusive jurisdiction of the London Court of International Arbitration. Any dispute, controversy, or claim arising out of or in connection with the support and maintenance contract, including any question regarding its existence, validity, interpretation, performance, breach, or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which Rules are deemed to be incorporated by reference into this clause. The seat (legal place) of arbitration shall be London, England. The number of arbitrators shall be 1 (one) arbitrator. The language of the arbitration shall be English. The governing law of the support and maintenance contract shall be the substantive law of laws of the Republic of Armenia

Appendix 2

Tender Invitation

Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

APPLICATION-STATEMENT

For participation in RFP

_____[Name of Bidder or in case of JV, insert legal name of each member]]

wishes to participate in the RFP with Reference Number CBA-2025-064, announced by the Central Bank of Armenia, and submits a proposal in accordance with the requirements of the Invitation.

We, the undersigned, declare and certify that:

1. We have reviewed the Invitation documents and have no reservations.
2. As of the date of submission of the bid, we meet the eligibility requirements set forth in the Invitation and, in accordance with clause 2.1 of the Invitation:

   a) We have not been declared bankrupt by a court and are not in the process of liquidation.

   b) During the previous five years, we have not been convicted of a crime involving the financing of terrorism, child exploitation or human trafficking, creating or participating in a criminal partnership, receiving a bribe, giving or brokering a bribe, or crimes against economic activity as prescribed by law, except in cases in where the conviction has been removed or extinguished in accordance with the law.

   c) We have not allowed and will not allow anti-competitive agreements, unfair competition, or abuse of dominant position during our participation in this procedure.

d) There is no simultaneous participation of any affiliated person, as defined in the Invitation, and/or organizations founded by us or in which we hold more than a fifty percent share.

Moreover, the declaration regarding actual beneficiaries is submitted in accordance with Appendix 2.1.

e) We are not included in the list of bidders who are not eligible to participate in the procurement process published in accordance with the procurement laws of member states of the Eurasian Economic Union.

f) We are not included in the list of bidders who are not eligible to participate in the procurement process.

3. Our proposal takes effect from the deadline for submission of proposals specified in the announcement and remains valid until the event specified in clause 9.4 of the Invitation.
4. If we are selected as the selected bidder, we undertake to provide contract security in accordance with the Invitation and to deliver the services within the timeframes specified in the Technical Task.
5. In accordance with clause 3.3 of this Invitation, we confirm that we are not submitting more than one proposal to this tender process.
6. We understand that this bid, if selected, constitutes a binding contract between us and the Purchaser until a formal contract is prepared and executed.

1) Name of Bidder:	*[insert Bidder's legal name], or [In case of JV, insert legal name of each member]*
2) Legal Address:	*[insert Bidder's legal address in country of registration], or [In case of JV, insert legal address in country of registration of each member]*
3) Business Address (if different):	*[insert Bidder's business address in country of registration], or [In case of JV, insert business address in country of registration of each member]*
4) Taxpayer Identification Number:	*[insert Bidder's Taxpayer identification number] or [In case of JV, insert Taxpayer identification number of each member]*
5) Phone Numbers:	
6) E-mail Address:	
7) Website:	

8) First Name and Last Name, Position, and Contact Information for Authorized Representative of Bidder:	
Copies of the following original documents are attached: " Organization Registration Documents " In the case of a joint venture, the JV agreement	

First Name and Last Name of Bidder's Principal:	
Position of Bidder's Principal:	
Signature of Above-Named Person	
Signing Date:	

Appendix 2.1

Tender Invitation

Reference Number: CBA-2025-064

DECLARATION REGARDING ACTUAL BENEFICIARIES

Information About Organization		
1.	Name	
2.	Registered/Legal Address	
3.	Business Address (if different)	
4.	Phone Number	
5.	E-mail Address	
6.	Website	
7.	First Name, Last Name, Position, Phone Number, and E-mail Address of Person Submitting the Declaration	
8.	First Name, Last Name, Position, Phone Number, and E-mail Address of Head(s) of Executive Body (with authority to sign in accordance with bidder's formation (charter) documents)	
9.	As of the date of submission of the bid, is the organization included in the list of persons not entitled to participate in the procurement process?	Yes □ No □
OWNERSHIP TYPE AND COMPOSITION OF OWNERS		
10	Co-Founded	Yes □

			No □		
	If yes, provide details, including information about shareholders holding 20% or more of the shares.				
	First Name, Last Name/Name	**Citizenship/Country of Registration**	**Date of Birth/ Date of State Registration**	**Passport Series, Number/ State Registration Number**	**Amount of Share Ownership**
	Private		Yes □ No □		
	If yes, provide information about shareholders holding 20% or more of the shares.				
	First Name, Last Name/Name	**Citizenship/Country of Registration**	**Date of Birth/ Date of State Registration**	**Passport Series, Number/ State Registration Number**	**Amount of Share Ownership**

INFORMATION ABOUT EXECUTIVE BODY

11.	Provide information about the members of the organization's executive body.				
	First Name, Last Name	**Citizenship**	**Date of Birth**	**Passport Series, Number**	**Position**

PERSONS WITH POLITICAL INFLUENCE[3]

12	Are there any persons with political influence among the owners or the executive body of the organization?	Yes □ No □			
	If yes, provide additional information:				
	First Name, Last Name	**Citizenship**	**Date of Birth**	**Passport Series, Number**	**Position**

DECLARATION REGARDING AFFILIATIONS[4]

13.	Are there any persons affiliated with any employee(s) of the Central Bank of Armenia among the owners or the executive body of the organization?	Yes □ No □			
	If yes, provide additional information:				
	First Name, Last Name	**Citizenship**	**Date of Birth**	**Passport Series, Number**	**Position**

DECLARATION REGARDING ACTUAL BENEFICIARIES

14	1. I, _____ _____ _____, as the _____ _____ of

[3] The definition of "persons with political influence" is provided in point 25 of part 1 of Article 3 of the RA Law on Combating Money Laundering and Terrorism Financing.

[4] Family members and persons closely related to them are considered "affiliated persons." "Family members" are blood relatives, spouses, or persons cohabitating in civil marriage. "Closely related" persons are persons who have social or professional ties with the person in question (e.g. friend, colleague, etc.).

	(first name, father's name, last name) (status) _____, declare that the actual beneficiary of the mentioned legal entity is: (name of organization) [redacted] : (first name, last name) a) _____ c) _____ (date of birth) (citizenship) b) _____ (passport series/number)
	2. The person listed in part 1 of the declaration is the actual beneficiary on the following basis/bases: ☐ the person is in fact acting on behalf of or for the benefit of the legal entity, or ☐ the person exercises actual (real) control over business relations between the legal entity and the Central Bank, or ☐ the person owns 20 or more percent of the voting shares (stakes) of the given legal entity or has a privileged opportunity to predetermine the legal entity's decisions by virtue of the person's participation or a contract executed with the legal entity, or is a member of the management and/or governing body of the legal entity, or acts in concordance with the legal entity based on common economic interests. ☐ Is there any affiliation between the actual beneficiary and any employee of the Central Bank of Armenia?

QUESTIONNAIRE ON THE ORGANIZATION'S PROCEDURES FOR COMPLIANCE WITH INTERNATIONAL SANCTIONS		
1	Does the organization have a compliance practice?	Yes ☐ No ☐

	If yes, please provide contact information: First Name, Last Name Position Tel. E-mail	
2	Does the organization have procedures aimed at complying with the requirements set forth in AML/CFT-related international sanctions lists?	Yes □ No □
3	Which international AML/CFT lists are used by the organization?	
4	How are compliance checks performed with regard to the lists mentioned in point 3 of this questionnaire?	Automatically □ Not automatically □
5	Does the organization, including branches or representative offices and subsidiaries, operate in countries considered high-risk from the point of view of ML/TF?[5]	
6	Has the organization had a business relationship with any individual or legal entity included in AML/CFT-related international sanctions lists?	Yes □ No □
	If yes, please provide detailed information on the nature of the business relationship, including the profits received and the types of transactions.	

I certify that the information provided in this declaration is true and correct.

First Name and Last Name:	

[5] The list of high-risk countries published by the FATF should be reviewed for a determination of which countries are considered high-risk in this sphere.

Signature:	
Signing Date:	

Appendix 3

Tender Invitation

Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

FINANCIAL PROPOSAL

Having examined the Tender Invitation with Reference Number CBA-2025-064, _[Name of Bidder] _____ offers to fulfill the contract at the total prices noted below.

[The Financial Proposal shall include the total cost of project implementation, as well as the expected post-implementation expenses over a ten-year period, including but not limited to the costs of software and software licenses, ongoing support and maintenance costs, and any other necessary expenses required by the Terms of reference, comprising the combined totals of Appendix 3.1 and Appendix 3.2.

The Armenian resident submits the financial proposal in AMD in accordance with clause 4.2 of this Invitation.

Non-resident Bidders of the Republic of Armenia shall be expressed in United States Dollar or Euro. In such case, for Proposal evaluation and comparison purposes all prices expressed in foreign currency will be converted into Armenian Dram (AMD). The conversion shall be conducted by the Purchaser, with the exchange rate announced at its official website "www.cba.am" by the Purchaser on the date of opening of Proposals. Moreover, a contract will be executed in the same currency as submitted in the proposal. In case of signing a contract with a non-resident Bidder of the Republic of Armenia, profit tax shall arise at the rate of twenty (20) percent of the contract price, payable by the Purchaser. The profit tax rate may be changed under a relevant Treaty for the Avoidance of Double Taxation between the countries of the Purchaser and the Bidder, in which case the successful Bidder shall provide the Purchaser with a Certificate of Residency, issued by the Tax Authority of its country, within ten (10) days of contract signature. If the supplier is subject to profit tax, the comparison of price proposals shall be carried out based on the total value including the profit tax.]

Lot	Purchase item	Price AMD, USD or EUR (in numbers and words)	VAT AMD, USD or EUR (in numbers and words) (if applicable)	Total Price AMD, USD or EUR (in numbers and words)
1	***2***	***3***	***4***	***5=3+4***
1	Real-Time Gross Settlement System	{in numbers}	{in numbers}	{in numbers}
		{in words}	{in words}	{in words}

_____ _____

Name of Bidder (position, first name and last name) Signature and stamp

Appendix 3.1

Tender Invitation

Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

BREAKDOWN OF FINANCIAL PROPOSAL

(Cost Breakdown Table for System Implementation)

[The Bidder shall submit a detailed breakdown of the System supply and implementation costs, clearly specifying the unit and total prices for each component. An advance payment may be granted only if the Bidder submits positive audited financial statements that meet the Purchaser's requirements (see ToR Section 9.4)]

Comp. Nr	Name	Brief description	Meas. Unit	Qty	Unit Price, incl. VAT (if appl.) /AMD, USD or EUR/	Total Price Incl. VAT (if appl.) /AMD, USD or EUR/
1	*2*	*3*	*4*	*5*	*6*	*7 =5x6*
1.1						
1.2						
…						

Detailed warranty service terms _____

Payment Terms _____

Payment Conditions _____

_____ _____

Name of Bidder (position, first name and last name) Signature and Stamp

Appendix 3.2

Tender Invitation

Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

BREAKDOWN OF FINANCIAL PROPOSAL

(Cost Breakdown Table for Post-Implementation recurring Costs)

[The Bidder shall provide a separate breakdown using Annex 3.2 of the expected post-implementation costs. The Bidder must outline the annual costs associated with support, maintenance and other required expenses of the deployed solution over a minimum period of 10 years. Clearly outline the payment terms, schedule, and procedures.

For each category, the Bidder shall also provide a 10-year cost projection, indicating key drivers of future cost changes in line with ToR Section 9.5.]

No	Name	The annual price of the service period per year					Total Prices
		Year 1	Year 2	Year 3	Year	Year 10	*AMD, USD or EUR*
1	.....						
2	.....						
3	.....						
4	.....						
Annual Subtotals:							
VAT (if applicable) /AMD, USD or EUR/							
Cumulative total cost of expected expenses							

Post-implementation recurring costs will be used exclusively for evaluation and comparison purposes in calculating the Total Cost of Ownership (TCO). A separate contract for the post-implementation period will be concluded after the implementation phase, taking into account the following terms:

- *Contract signed for a minimum of ten (10) years;*
- *Fixed pricing for the first three (3) years;*
- *The agreed procedure and frequency of price reviews for each next 3 years, including 20% adjustment limits.*

Terms, schedule, and method of payment _____

Detailed terms of post-warranty service _____

_____ _____

Name of Bidder (position, first name and last name) Signature and Stamp

In addition to Appendices 3, 3.1, and 3.2, the bidder shall submit a completed detailed cost breakdown in XLS.

Appendix 4

Tender Invitation

Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

COMPREHENSIVE DESCRIPTION

of the Proposed Solution

_____[Name of Bidder]_____ presents below a comprehensive description of the Solution proposed by bidder within the framework of the Tender with Reference Number CBA-2025-064 , broken down by component.

The Bidder shall structure the technical part of its Proposal in line with the Terms of Reference (Appendix 1), explicitly covering all chapters.

For each requirement, the Bidder shall clearly indicate compliance, partial compliance or non-compliance and provide supporting explanations.

The technical proposal shall also include: an implementation RACI matrix in line with ToR Section 11, a cutover and rollback strategy aligned with the CBA's operational requirements, and a high-level Business Continuity and Disaster Recovery concept consistent with ToR Chapter 8 and Chapter 6.

A detailed description of the proposed solution shall contain the following populated Vendor Response documents and use file name "CBA-2025-064_Appendix_4":

- Documents describing the proposed solution (e.g. Architecture Diagrams, Integration Diagrams, Project Plans, User Guides) using file names "CBA-2025-064_Appendix_4_Attachment _[dd]" where [dd] reflects a sequential number used to uniquely identifying each document.
- Implementation timeline showing durations and key milestones
- Any other documents and information specified in Terms of Reference of this Invitation,

Note that for certain requirements stated in .xlsx documents, respondents are asked to select their Delivery Approach. A selection must be done in column "Delivery Approach" when the current selected value states "(Please select from below)*". The respondent can select between the following values:

- *Requires product development* – to be used when the current product does not support the requirement and the Respondent intends to develop and include the required functionality as part of future product development. Example: the product does not support the manual entry of payment messages and the Respondent plans to add this functionality in a future release.
- *Requires customization for CBA* – to be used when the current product partially supports the requirement, and the Respondent plans to deliver the required functionality through customization of the existing product. Example: the product supports manual entry of payment messages but does not implement the 4-eyes principle, which the Respondent plans to add as a customization for CBA.
- *Comes out of the box / configuration* – to be used when the requirement is fulfilled by functionality that is readily available in the product or can be implemented through standard configuration.

Further explanations shall be provided in the "Vendor Response" column. The Respondent may refer to additional documents included in its submission (please refer to cipher e) above), by specifying the file name in the "Attachment Name" column. If multiple documents are referenced, the file names shall be separated by commas.

Attachment Name	Content Description

Appendix 5

Tender Invitation
Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

INFORMATION

About the Bidder's "Professional experience"

[In addition to the minimum participation requirements and minimum qualification requirements defined in Part 2 of this Invitation, the Bidder must also meet the qualification criteria set out in the Terms of Reference.

Bidders shall demonstrate proven experience in the design and implementation of RTGS solutions for central banks, for at least 5 (five) years.

The submitted portfolio shall include information on successfully implemented systems within the last 5 (five) years prior to the submission date.

The bidder must have successfully completed at least 3 (three) contracts of a similar nature and scope within the last 10 years. The bidder must have at least 3 (three) existing support & maintenance contract.

The Bidder shall also provide Client confirmation or supporting reference materials (e.g., reference letters, project briefs, regulator acknowledgements, or publicly available information) validating successful completion.]

№	Name of Partner Organization and country	Project scope and key objectives / Brief Description	Implementation timeline and duration Month/Year	Main solution components and technologies used	Dedicated team/team size in the whole Project	Approximate contract price/AMD, USD or EUR/	Contacts of the Partner Organization
1.							Contact person: Position: Address: Email: Telephone:
2.							Contact person: Position: Address: Email: Telephone:
3.							Contact person: Position: Address: Email: Telephone:

Appendix 6

Tender Invitation

Reference Number: CBA-2025-064

Note: All italicized text in blue colour is for use in preparing this form and shall be deleted from the final product.

INFORMATION

About the Bidder's "Human Resources"

[The Bidder shall provide an Organizational and Governance Overview that includes the organizational structure of the proposed account management and project team, CVs or profiles of key personnel, a description of the governance and decision-making framework (including escalation and communication procedures), and examples of similar client engagement models implemented for other central banks or financial institutions.

The Bidder shall assign qualified and experienced personnel to perform the required tasks and ensure the achievement of the Contract objectives in terms of both timeline and quality. All personnel involved in the project implementation must possess the necessary qualifications and demonstrated experience in similar projects to ensure high-quality performance.]

Key Personnel						
Nr.	**Name**	**Role/Position**	**Main functions**	**Educational Background**	**Total Experience (in Years)**	**Number of years within your Organization**
1						
2						
3						

** As evidence, the Bidder must submit the CVs of key personnel (including supporting documentation confirming their qualifications), clearly indicating their relevant work experience and number of years in each role. All team members must have at least working proficiency in English or Armenian (knowledge of Russian is desirable).*

Where Bidders submit personal data as part of their Proposal (e.g., CVs, diplomas, certificates), the Central Bank of Armenia will process such data solely for the purposes of conducting and evaluating this procurement procedure and performing any resulting contractual obligations.

The CBA will handle personal data lawfully, fairly, and securely, ensuring its confidentiality and using it only for purposes related to this procedure. Personal data will be retained only for the statutory period required for procurement records and will be securely deleted or archived thereafter.

By submitting such data, the Bidder confirms that it has obtained all necessary permissions or has a valid legal basis for providing this personal data to the CBA.

Key Personnel Details

<table>
<tr><td colspan="2">Position</td><td colspan="3">Candidate

☐ Prime ☐ Alternate</td></tr>
<tr><td rowspan="5">Personnel information</td><td colspan="4">Name</td></tr>
<tr><td colspan="4">Educational Background, Professional qualifications, Training / Certification including institutions, specialization areas etc.</td></tr>
<tr><td>Degree/Certificates etc.</td><td colspan="2">Year of Award</td><td>University/other</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="4">Present employment</td><td colspan="4">Name of Employer</td></tr>
<tr><td colspan="4">Address of Employer</td></tr>
<tr><td colspan="3">Telephone, E-mail</td><td></td></tr>
<tr><td colspan="3">Years with present Employer</td><td></td></tr>
</table>

Summarize professional experience over the last five - ten years, in reverse chronological order.

From	To	Company / Project / Position / Relevant technical and management experience